

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-175605

(43)Date of publication of application : 29.06.2001

(51)Int.Cl.
 G06F 15/00
 G10L 11/00
 H04H 1/00
 H04L 9/10
 H04N 7/167
 H04N 7/173

(21)Application number : 11-359896

(71)Applicant : SONY CORP

(22)Date of filing : 17.12.1999

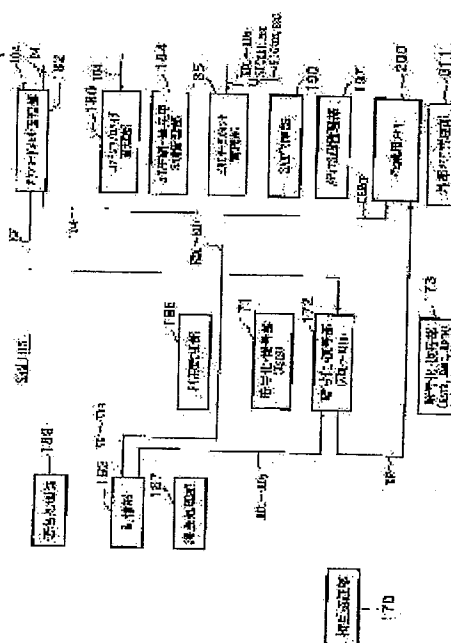
(72)Inventor : NONAKA SATOSHI
EZAKI TADASHI

(54) DATA PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data processor which can effectively protect the profit of a provider of content data.

SOLUTION: Secure container 104 containing content data ciphered by using content key data, the mentioned ciphered content key data, and title deed data showing the handling of the content data is inputted from a content provider management part 180, and a charging process part 187 determines at least one of the purchase style and use style of the content data according to the handling that the title deed data indicate. The charging process part 187 generates history data showing the result of the mentioned decision. Each process part is stored in a tamper-resisting circuit module.



【特許請求の範囲】

【請求項 1】コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項 2】前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項 1 に記載のデータ処理装置。

【請求項 3】前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する請求項 2 に記載のデータ処理装置。

【請求項 4】前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する請求項 2 に記載のデータ処理装置。

【請求項 5】前記記録媒体がセキュア RAM 領域を有する場合に、前記権利書データおよび前記暗号化された前記利用制御データを前記セキュア RAM 領域に記録するように制御する記録制御手段を前記耐タンパ性の回路モジュール内にさらに有する請求項 4 に記載のデータ処理装置。

【請求項 6】前記記録媒体が相互認証機能を持つ耐タンパ性のデータ処理装置を有する場合に、前記権利書データおよび前記暗号化された前記利用制御データを前記記録媒体の前記データ処理装置に記録するように制御する記録制御手段を前記耐タンパ性の回路モジュール内にさらに有する請求項 4 に記載のデータ処理装置。

【請求項 7】前記履歴データ生成手段は、前記コンテンツデータを提供したデータ提供装置の識別子、ユーザの識別子、

当該データ処理装置の識別子、当該コンテンツデータに係わるライセンス所有者の識別子を少なくとも記述した

前記履歴データを生成する請求項 1 に記載のデータ処理装置。

【請求項 8】前記利用制御データ生成手段は、前記購入形態を決定したユーザの識別子および前記決定された購入形態を少なくとも記述した前記利用制御データを生成する請求項 2 に記載のデータ処理装置。

【請求項 9】前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらにを行い、

10 前記データ処理装置は、

前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項 1 に記載のデータ処理装置。

【請求項 10】前記署名データは、前記コンテンツ鍵データおよび前記権利書データの作成者の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記作成者の公開鍵データを用いて前記署名データの正当性を検証する請求項 9 に記載のデータ処理装置。

【請求項 11】前記署名データは、前記コンテンツ鍵データおよび前記権利書データの送り元の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記送り元の公開鍵データを用いて前記署名データの正当性を検証する請求項 9 に記載のデータ処理装置。

【請求項 12】前記入力処理手段は、前記コンテンツデータの署名データを入力する処理をさらにを行い、

30 前記データ処理装置は、

前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項 1 に記載のデータ処理装置。

【請求項 13】前記入力処理手段は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて秘密鍵データを用いて作成された署名データと、前記秘密鍵データに対応する公開鍵データとを入力する処理をさらにを行い、

40 前記データ処理装置は、

前記公開鍵データを用いて、前記署名データの正当性を検証する署名処理手段を前記耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項 1 に記載のデータ処理装置。

【請求項 14】前記コンテンツ鍵データは、ライセンス鍵データを用いて暗号化されており、前記データ処理装置は、

前記ライセンス鍵データを記憶する記憶手段をさらに有し、

前記復号手段は、前記記憶手段から読み出した前記ライセンス鍵データを用いて前記コンテンツ鍵データを復号する請求項1に記載のデータ処理装置。

【請求項15】前記データ処理装置は、他の装置との間で、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一のデータをオンラインで送受信する場合に、前記他の装置との間で相互認証を行う相互認証手段と、

前記相互認証によって得られたセッション鍵データを用いて、前記送受信を行うデータの暗号化および復号を行う暗号化・復号手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項1に記載のデータ処理装置。

【請求項16】前記データ処理装置は、他の装置との間でデータの送受信を行う際に、無効にされた装置のリストを記述したリボケーションリストを参照し、当該リボケーションリストに前記他の装置が無効であることが示されていない場合に、前記他の装置との間でデータの送受信を行う請求項15に記載のデータ処理装置。

【請求項17】コンテンツデータの提供をデータ提供装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項18】前記入力処理手段は、前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う請求項17に記載のデータ処理装置。

【請求項19】前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データを格納したキーファイルとを入力する処理を行う請求項18に記載のデータ処理装置。

【請求項20】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項19に記載のデータ処理装置。

【請求項21】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項20に記載のデータ処理装置。

【請求項22】前記入力処理手段は、

前記コンテンツファイルの作成者および送り主である前記データ提供装置の第1の署名データと、前記キーファイルの作成者である前記管理装置の第2の署名データと、前記キーファイルの送り主である前記データ提供装置の第3の署名データとをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記第1の署名データ、前記第2の署名データおよび前記第3の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記第1の署名データ、前記第2の署名データおよび前記第3の署名データの正当性が確認された後に、前記決定を行う請求項19に記載のデータ処理装置。

【請求項23】前記第1の署名データおよび前記第3の署名データは、前記データ提供装置の秘密鍵データを用いて作成されており、

前記第2の署名データは、前記管理装置の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記データ提供装置の公開鍵データを用いて前記第1の署名データおよび前記第3の署名データの検証を行い、前記管理装置の公開鍵データを用

いて前記第2の署名データの検証を行う請求項22に記載のデータ処理装置。

【請求項24】前記入力処理手段は、前記データ提供装置の秘密鍵データに対応する公開鍵データをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記署名処理手段は、前記モジュールに格納された公開鍵データを用いて、前記第1の署名データおよび前記第3の署名データの検証を行う請求項23に記載のデータ処理装置。

【請求項25】前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールの入力処理を行い、

前記データ処理装置は、

前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する請求項18に記載のデータ処理装置。

【請求項26】コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項27】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツデータの購入形態の決定処理が行われる

際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項28】前記入力処理手段は、

前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う請求項27に記載のデータ処理装置。

【請求項29】前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データを格納したキーファイルと、前記価格データとを入力する処理を行う請求項28に記載のデータ処理装置。

【請求項30】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項29に記載のデータ処理装置。

【請求項31】前記入力処理手段は、

前記コンテンツファイルの作成者および送り主である前記データ提供装置の第1の署名データと、前記コンテンツファイルの送り主である前記データ配給装置の第2の署名データと、前記キーファイルの作成者である前記管理装置の第3の署名データと、前記キーファイルの送り主である前記データ提供装置の第4の署名データと、前記キーファイルの送り主である前記データ配給装置の第5の署名データと、前記価格データの作成者および送り主である前記データ配給装置の第6の署名データをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記第1の署名データ、前記第2の署名データ、前記第3の署名データ、前記第4の署名データ、前記第5の署名データおよび前記第6の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記第1の署名データ、前記第2の署名データ、前記第3の署名データ、前記第4の署名データ、前記第5の署名データおよび第6の署名データの正当性が確認された後に、前記

決定を行う請求項 28 に記載のデータ処理装置。

【請求項 32】前記第 1 の署名データおよび前記第 4 の署名データは、前記データ提供装置の秘密鍵データを用いて作成されており、

前記第 2 の署名データ、前記第 5 の署名データおよび前記第 6 の署名データは、前記データ配給装置の秘密鍵データを用いて作成されており、

前記第 3 の署名データは、前記管理装置の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記データ提供装置の公開鍵データを用いて前記第 1 の署名データおよび前記第 4 の署名データの検証を行い、前記データ配給装置の公開鍵データを用いて前記第 2 の署名データ、前記第 5 の署名データおよび前記第 6 の署名データの検証を行い、前記管理装置の公開鍵データを用いて前記第 3 の署名データの検証を行う請求項 31 に記載のデータ処理装置。

【請求項 33】前記入力処理手段は、前記データ提供装置の秘密鍵データに対応する公開鍵データと、前記データ配給装置の秘密鍵データに対応する公開鍵データとをさらに格納した前記モジュールを入力する処理を行い、前記データ処理装置は、

前記署名処理手段は、前記モジュールに格納された前記データ提供装置の公開鍵データを用いて前記第 1 の署名データおよび前記第 4 の署名データの検証を行い、前記モジュールに格納された前記データ配給装置の公開鍵データを用いて前記第 2 の署名データ、前記第 5 の署名データおよび前記第 6 の署名データの検証を行う請求項 32 に記載のデータ処理装置。

【請求項 34】前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する請求項 28 に記載のデータ処理装置。

【請求項 35】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項 36】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対する課金処理を行う第 1 の処理モジュールと、

前記受信したモジュールに格納された前記権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納された前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを有する耐タンパ性の第 2 の処理モジュールとを有するデータ処理装置。

【請求項 37】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、

当該データ処理装置の秘密鍵データを記憶する記憶回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場

合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項38】前記前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路をさらに有し、

前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う請求項37に記載のデータ処理装置。

【請求項39】前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路とをさらに有する請求項37に記載のデータ処理装置。

【請求項40】前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する請求項37に記載のデータ処理装置。

【請求項41】記録媒体に搭載された相互認証機能を持つデータ処理回路、半導体記憶回路およびICカードの少なくとも一つとの間で通信を行うインターフェイスをさらに有する請求項37に記載のデータ処理装置。

【請求項42】有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、

前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、

前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、

前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する請求項37に記載のデータ処理装置。

【請求項43】前記公開鍵暗号回路、前記共通鍵暗号回路および前記ハッシュ関数回路のうち少なくとも一つの回

路を、前記記憶回路に記憶されたプログラムを前記演算処理回路で実行して実現する請求項37に記載のデータ処理装置。

【請求項44】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、

当該データ処理装置の秘密鍵データを記憶する記憶回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データに対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスとを有する耐タンパ性の回路モジュールと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項45】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化の際に用いる鍵データを記憶する記憶回路と、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項46】前記記憶回路は、前記記録領域に記録されるコンテンツデータがコンテンツ鍵データを用いて暗号化されている場合に、暗号化された前記コンテンツ鍵データを記憶する請求項45に記載のデータ処理装置。

【請求項47】前記記憶回路は、前記記録領域に記録されるコンテンツデータの取り扱いを示す権利書データを記憶する請求項46に記載のデータ処理装置。

【請求項48】前記記憶回路は、他の装置と通信を行う際に当該装置の有効性を判断する情報を示すリボケーションリストを記憶し、

前記演算処理回路は、前記リボケーションリストに基づいて、前記他の装置が無効であると判断した場合に、前記他の装置との間の通信を停止する請求項45に記載のデータ処理装置。

【請求項49】前記記録媒体の記録領域がROM型であり、当該記録領域にコンテンツ鍵データで暗号化されたコンテンツデータが記録されている場合に、

前記記憶回路は、初期状態で、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを記憶している請求項45に記載のデータ処理装置。

【請求項50】前記記録媒体の記録領域がRAM型である場合に、

前記記憶回路は、前記記録領域にコンテンツ鍵データで暗号化されたコンテンツデータが記録される際に、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを記憶する請求項45に記載のデータ処理装置。

【請求項51】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項52】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

10 当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と外部インターフェイスと、

演算処理回路と、

20 前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項53】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

外部インターフェイスとを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項54】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

40 当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

外部インターフェイスと、

演算処理回路と、

50 前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の

回路モジュール内に有するデータ処理装置。

【請求項55】ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化の際に用いる鍵データとを記憶する記憶回路と、

他の装置が秘密鍵データを用いて作成した署名データに対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、外部インターフェイスとを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路の制御を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項56】コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、

前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項57】前記データの伸長が部分的に行われるように制御する半開示制御回路をさらに有する請求項56に記載のデータ処理装置。

【請求項58】前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路をさらに有する請求項56に記載のデータ処理装置。

【請求項59】コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツデータに対応して入力したソフトウェアに基づいて、前記コンテンツデータの圧縮および伸長の少なくとも一方と、前記圧縮および伸長の対象となるコンテンツデータに対して電子透かし情報の検出および埋め込みを行う演算処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項60】ROM型またはRAM型の記録媒体にア

クセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項61】前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路をさらに有する請求項60に記載のデータ処理装置。

【請求項62】前記データ処理装置の識別子を記憶する記憶回路と、

前記データ処理装置の識別子および前記記録媒体の識別子に基づいて前記記録媒体にユニークな記録用鍵データを生成する記録用鍵データ生成回路とをさらに有し、前記共通鍵暗号回路は、前記記録用鍵データを用いて、前記記録媒体に記録されるコンテンツデータの暗号化および復号を行う請求項61に記載のデータ処理装置。

【請求項63】ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項64】ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用

いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項65】ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、提供されたコンテンツデータに関連する処理を行うデータ処理装置に関する。

【0002】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このようなデータ提供システムの一つに、音楽データを配信する従来のEMD (Electronic Music Distribution: 電子音楽配信) システムがある。

【0003】図109は、従来のEMDシステム700の構成図である。図109に示すEMDシステム700では、コンテンツプロバイダ701a、701bが、サービスプロバイダ710に対し、コンテンツデータ704a、704b、704cと、著作権情報705a、705b、705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、

あるいはオフラインで供給する。ここで、著作権情報705a、705b、705cには、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】サービスプロバイダ710は、受信したコンテンツデータ704a、704b、704cと、著作権情報705a、705b、705cとをセッション鍵データを用いて復号する。そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a、704b、704cに、著作権情報705a、705b、705cを埋め込んで、コンテンツデータ707a、707b、707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a、705b、705cのうち電子透かし情報をコンテンツデータ704a、704b、704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。さらに、サービスプロバイダ710は、コンテンツデータ707a、707b、707cを、鍵データベース706から読み出したコンテンツ鍵データKca、Kcb、Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a、707b、707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA (Conditional Access) モジュール711に送信する。

【0005】CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca、Kcb、Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a、707b、707cを、それぞれコンテンツ鍵データKca、Kcb、Kccを用いて復号することが可能になる。このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約 (更新) 情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービス

プロバイダ 710 とコンテンツプロバイダ 701a, 701b, 701c との間で利益配分を行う。このとき、サービスプロバイダ 710 から、コンテンツプロバイダ 701a, 701b, 701c への利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRAC によって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】また、端末装置 709 では、コンテンツ鍵データ Kca, Kcb, Kcc を用いて復号したコンテンツデータ 707a, 707b, 707c を、RAM 型の記録媒体 723 などに記録する際に、著作権情報 705a, 705b, 705c の SCMS ビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ 707a, 707b, 707c に埋め込まれた SCMS ビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】ところで、SCMS は、コンテンツデータを例えば 2 世代以上のわたって複製することを禁止するものであり、1 世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【0009】また、上述した EMD システム 700 では、サービスプロバイダ 710 が暗号化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ 701 の関係者はサービスプロバイダ 710 の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ 701 の利益が不当に損なわれる可能性が高いという問題がある。また、上述した EMD システム 700 では、ユーザの端末装置 709 がサービスプロバイダ 710 から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ 701 の利益が不当に損なわれるという問題がある。

【0010】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護することを可能にするデータ処理装置を提供することを目的とする。また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ処理装置を提供することを目的とする。

【0011】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第 1 の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された

前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0012】本発明の第 1 の観点のデータ処理装置の作用を以下に示す。例えば、コンテンツデータを提供するデータ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとが、入力手段に入力される。次に、決定手段によって、ユーザによるコンテンツデータの購入形態および利用形態を決定する操作に応じて、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。すなわち、ユーザによるコンテンツデータの決定は、権利書データが示すコンテンツデータの取り扱いに従って行われる。この場合に、データ提供装置の関係者が権利書データを作成することで、当該関係者がコンテンツデータの購入および利用を制御できる。次に、履歴データ生成手段によって、前記決定の結果を示す履歴データが生成される。当該履歴データは、例えば、コンテンツデータの利用等に伴って得られた利益を関係者に分配する管理装置に送られる。また、当該第 1 の観点のデータ処理装置では、復号手段によって、前記コンテンツ鍵データを復号が行われる。すなわち、耐タンパ性の回路モジュール内で、コンテンツ鍵データの復号を行うことで、所定の購入形態の決定処理を経た後にのみ、コンテンツ鍵データを用いたコンテンツデータの復号を可能にすることができ、コンテンツデータの不正使用を効果的に阻止できる。

【0013】また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段とを前記耐タンパ性の回路モジュール内にさらに有する。

【0014】また、本発明の第 1 の観点のデータ処理装置は、好ましくは、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する。

【0015】また、本発明の第 1 の観点のデータ処理装

置は、好ましくは、前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらにを行い、前記データ処理装置は、前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う。

【0016】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、他の装置との間でデータの送受信を行う際に、無効にされた装置のリストを記述したリボケーションリストを参照し、当該リボケーションリストに前記他の装置が無効であることが示されていない場合に、前記他の装置との間でデータの送受信を行う。

【0017】また、本発明の第2の観点のデータ処理装置は、コンテンツデータの提供をデータ提供装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0018】本発明の第2の観点のデータ処理装置の作用を説明する。入力処理手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理が行われる。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。次に、出力手段において、前記履歴データが前記管理装置に出力される。

【0019】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う。

【0020】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテ

ンツ鍵データおよび前記権利書データを格納したキーファイルとを入力する処理を行う。

【0021】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールの入力処理を行い、前記データ処理装置は、前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する。

【0022】また、本発明の第3の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0023】本発明の第3の観点のデータ処理装置の作用を説明する。入力処理手段において、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールが所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力される。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、復号手段において、前記コンテンツ鍵データが復号される。

【0024】また、本発明の第4の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記

決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0025】本発明の第4の観点のデータ処理装置の作用を説明する。入力手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理が行われる。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、出力手段によって、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データが出力される。また、出力手段によって、前記履歴データが前記管理装置に出力される。また、復号手段において、前記コンテンツ鍵データが復号される。

【0026】また、本発明の第4の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う。

【0027】また、本発明の第4の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データを格納したキーファイルと、前記価格データとを入力する処理を行う。

【0028】また、本発明の第5の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツファイルの作成者および送り主である前記データ提供装置の第1の署名データと、前記コンテンツファイルの送り主である前記データ配給装置の第2の署名データと、前記キーファイルの作成者である前記管理装置の第3の署名データと、前記キーファイルの送り主である前記データ提供装置の第4の署名データと、前記キーファイルの送り主である前記データ配給装置の第5の署名データと、前記価格データの作成者および送り主である前記データ配給装置の第6の署名データをさらに格納した前記モジュールを入力する処理を行い、前記データ処理装置は、前記第1の署名データ、前記第2の署名データ、前記第3の署名データ、前記第4の署名データ、前記第5の署名データおよび前記第6の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、前記決定手段は、前記署名処理手段によって前記第1の署名データ、前記第2の署名データ、前記第3の署名データ、前記第4の署名データ、前

記第5の署名データおよび第6の署名データの正当性が確認された後に、前記決定を行う。

【0029】また、本発明の第6の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0030】本発明の第6の観点のデータ処理装置の作用を説明する。入力処理手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力される。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、出力手段において、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データが出力されると共に、前記履歴データが前記管理装置に出力される。また、復号手段において、前記コンテンツ鍵データが復号される。

【0031】また、本発明の第7の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについ

て付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第1の処理モジュールを有する。また、当該第7の観点のデータ処理装置は、前記受信したモジュールに格納された前記権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納された前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを有する耐タンパ性の第2の回路モジュールを有する。

【0032】本発明の第8の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によ

って得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有する。

【0033】また、本発明の第8の観点のデータ処理装置は、好ましくは、前記前記コンテンツデータ、前記コ

ンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路をさらに有し、前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う。

【0034】また、本発明の第8の観点のデータ処理装置は、好ましくは、前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路とをさらに有する。

【0035】また、本発明の第8の観点のデータ処理装置は、好ましくは、前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する。

【0036】また、本発明の第8の観点のデータ処理装置は、好ましくは、有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する。

【0037】また、本発明の第8の観点のデータ処理装置は、好ましくは、前記公開鍵暗号回路、前記共通鍵暗号回路および前記ハッシュ関数回路のうち少なくとも一つの回路を、前記記憶回路に記憶されたプログラムを前記演算処理回路で実行して実現する。

【0038】また、本発明の第9の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認

証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスとを有する耐タンパ性の回路モジュールと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【0039】また、本発明の第10の観点のデータ処理装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【0040】また、本発明の第10の観点のデータ処理装置は、好ましくは、前記記憶回路は、前記記録領域に記録されるコンテンツデータがコンテンツ鍵データを用いて暗号化されている場合に、暗号化された前記コンテンツ鍵データを記憶する。

【0041】また、本発明の第10の観点のデータ処理装置は、好ましくは、前記記憶回路は、他の装置と通信を行う際に当該装置の有効性を判断する情報を示すリボケーションリストを記憶し、前記演算処理回路は、前記リボケーションリストに基づいて、前記他の装置が無効であると判断した場合に、前記他の装置との間の通信を停止する。

【0042】また、本発明の第11の観点のデータ処理装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との

間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【0043】また、本発明の第12の観点のデータ処理装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【0044】また、本発明の第13の観点のデータ処理装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスとを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【0045】また、本発明の第14の観点のデータ処理装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【0046】また、本発明の第15の観点のデータ処理

装置は、ROM型あるいはRAM型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化の際に用いる鍵データを記憶する記憶回路と、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、外部インターフェイスと、を有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路の制御を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【0047】また、本発明の第16の観点のデータ処理装置は、コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有する。

【0048】また、本発明の第16の観点のデータ処理装置は、好ましくは、前記データの伸長が部分的に行われるように制御する半開示制御回路をさらに有する。

【0049】また、本発明の第17の観点のデータ処理装置は、ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。

【0050】また、本発明の第17の観点のデータ処理装置は、好ましくは、前記データ処理装置の識別子を記憶する記憶回路と、前記データ処理装置の識別子および前記記録媒体の識別子に基づいて前記記録媒体にユニークな記録用鍵データを生成する記録用鍵データ生成回路とをさらに有し、前記共通鍵暗号回路は、前記記録用鍵データを用いて、前記記録媒体に記録されるコンテンツデータの暗号化および復号を行う。

【0051】また、本発明の第18の観点のデータ処理

装置は、ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。

【0052】また、本発明の第19の観点のデータ処理装置は、ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【0053】また、本発明の第20の観点のデータ処理装置は、ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【0054】

【発明の実施の形態】以下、本発明の実施形態に係わるEMD(Electronic Music Distribution: 電子音楽配信)システムについて説明する。

第1実施形態

図1は、本実施形態のEMDシステム100の構成図で

ある。本実施形態において、ユーザに配信されるコンテンツ(Content)データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM1051~1054が、本発明のデータ提供装置、管理装置およびデータ処理装置にそれぞれ対応している。まず、EMDシステム100の概要について説明する。EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データKc、コンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

【0055】EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データKc、権利書データ106並びに電子透かし情報鍵データを登録(認証および権威化)する。また、EMDサービスセンタ102は、対応する期間のライセンス鍵データKD1~KD56で暗号化したコンテンツ鍵データKc、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

【0056】また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテンツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ(本発明のモジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0057】ユーザホームネットワーク103は、例えば、ネットワーク機器1601およびAV機器1602~1604を有する。ネットワーク機器1601は、SAM(Secure Application Module)1051を内蔵している。AV機器1602~1604は、それぞれSAM

1052~1054を内蔵している。SAM1051~1054相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0058】SAM1051~1054は、ネットワーク機器1601がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および/または、コンテンツプロバイダ101からAV機器1602~1604に記録媒体を介してオフラインで供給されたセキュアコンテナ104を対応する期間のライセンス鍵データKD1~KD3を用いて復号した後に、署名データの検証を行う。SAM1051~1054に供給されたセキュアコンテナ104は、ネットワーク機器1601およびAV機器1602~1604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM1051~1054は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録すると共に、購入形態を示す利用制御データ166を作成する。利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。利用制御データ166は、例えば、購入形態が決定される度に、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0059】EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0060】本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての(ルート認証局92の下層に位置する)セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM1051~1054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権

利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。また、EMDサービスセンタ102は、例えば、ライセンス鍵データKD₁～KD₆などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price)とSAM105₁～SAM105₄から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

【0061】図2は、セキュアコンテナ104の概念をまとめた図である。図2に示すように、セキュアコンテナ104には、コンテンツプロバイダ101が作成したコンテンツファイルCFと、EMDサービスセンタ102が作成したキーファイルKFとが格納されている。コンテンツファイルCFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、コンテンツ鍵データK_cを用いた暗号化されたコンテンツデータCと、これらについて

のコンテンツプロバイダ101の秘密鍵データK_{CP,S}を用いた署名データとが格納されている。キーファイルKFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、ライセンス鍵データKD₁～KD₆によって暗号化されたコンテンツ鍵データK_cおよび権利書データ106と、これらについてのEMDサービスセンタ102の秘密鍵データK_{ESC,S}による署名データとが格納されている。なお、図2において、権利書データ106は、ライセンス鍵データによって暗号化されていなくてもよい。但し、この場合でも、権利書データ106

には、コンテンツプロバイダ101の秘密鍵データK_{CP,S}を用いた署名データを付加する。

【0062】以下、EMDシステム100の各構成要素について詳細に説明する。

【コンテンツプロバイダ101】コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データK_{CP,P}、自らの身分証明書および銀行口座番号(決済を行う口座番号)をオフラインでEMDサービスセンタ102に登録し、自らの識別子(識別番号)CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データK_{ESC,P}と、ルート認証局92の公開鍵データK_{R-CA,P}とを受ける。

【0063】コンテンツプロバイダ101は、図3(A)に示すコンテンツファイルCFと、当該コンテンツファイルCFの署名データSIG_{6,CP}と、キーファイルデータベース118bから読み出した当該コンテンツファイルCFに対応する図3(B)に示すキーファイルKFと、当該キーファイルKFの署名データSIG_{7,CP}

と、記憶部119から読み出したコンテンツプロバイダ101の公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}の署名データSIG_{1,ESC}とを格納したセキュアコンテナ104を生成する。また、コンテンツプロバイダ101は、セキュアコンテナ104をオンラインあるいはオフラインで、図1に示すユーザホームネットワーク103のネットワーク機器1601に供給する。このように、本実施形態では、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}をセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band)方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CER_{CP}を得るための通信をEMDサービスセンタ102との間で行う必要がない。なお、本発明では、公開鍵証明書CER_{CP}をセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書CER_{CP}を得るアウト・オブ・バンド(Out-Of-band)方式を採用してもよい。

【0064】なお、本実施形態では、署名データは、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁～105₄の各々において、署名を行なう対象となるデータのハッシュ値をとり、自らの秘密鍵データK_{CP,S}、K_{ESC}、K_{SAM1}～K_{SAM4}を用いて作成される。ここで、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値(出力)から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0065】以下、セキュアコンテナ104内の各データについて詳細に説明する。

<署名データSIG_{6,CP}>署名データSIG_{6,CP}は、セキュアコンテナ104の受信先において、コンテンツファイルCFの作成者および送信者の正当性を検証するために用いられる。

<署名データSIG_{7,CP}>署名データSIG_{7,CP}は、セキュアコンテナ104の受信先において、キーファイルKFの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ104の受信先において、キーファイルKFの作成者の正当性の検証は、キーファイルKF内の署名データSIG_{K1,ESC}に基づいて行われる。また、署名データSIG_{K1,ESC}は、キーファイルKFが、EMDサービスセンタ102に登録されているか否かを検証するためにも用いられる。

【0066】<コンテンツファイルCF>図4は、図3(A)に示すコンテンツファイルCFをさらに詳細に説

明するための図である。コンテンツファイルCFは、図3(A)および図4に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたメタデータMeta、コンテンツデータC、A/V伸長用ソフトウェアSoftおよび電子透かし情報モジュール(Watermark Module)WMとを格納している。なお、図3(A)は、コンテンツデータCを伸長するAV圧縮伸長用装置として、DSP(Digital Signal Processor)を用いた場合のコンテンツファイルCFの構成である。当該DSPでは、セキュアコンテナ104内のA/V伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ104内のコンテンツデータCの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ101は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。AV圧縮伸長用装置としてA/V伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルCF内にA/V伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0067】ヘッダデータには、図4に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データKcp.sによる署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルCFの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関する情報、およびディレクトリ情報などに関するコンテンツプロバイダ101の秘密鍵データKcp.sによる署名データが含まれる。

【0068】メタデータMetaには、図4に示すように、商品(コンテンツデータC)の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。本発明では、図3(A)および図4に示すように、コンテンツファイルCF内にメタデータMetaを格納して送信する場合を例示するが、メタデータMetaをコンテンツファイルCF内に格納せずに、コンテンツファイルCFを送信する経路とは別の経路でコンテンツプロバイダ101からSAM1051などに送信してもよい。

【0069】コンテンツデータCは、例えば、コンテンツマスタソースデータベースから読み出したコンテンツデータに対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wc、ユーザ電子透かし情報(User Watermark)Wuおよびリンク用電子透かし情報(Link Watermark)WLなどを埋め込んだ後に、例えば、ATRAC3(Adaptive Transform Acoustic Coding 3)(商標)などの音声圧縮方式で圧縮され、その後、コンテンツ鍵データK

cを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で暗号化されたデータである。ここで、コンテンツ鍵データKcは、例えば、乱数発生器を用いて所定ビット数の乱数を発生して得られる。なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテンツプロバイダ101によって固有のコンテンツ鍵データKcを用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データKcを用いてもよい。

【0070】ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM1051~1054の識別子SAM_ID1~SAM_ID4が含まれる。リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配信された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなわち、当該コンテンツデータCの受信先において、電子透かし情報デコーダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

【0071】具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD(Mini Disk)などの光ディスクなどの可搬メディアに搭載されているメディアSAM

に記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【0072】なお、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ302は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

【0073】また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器1601およびAV機器1602～1604が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク103では、EMDサービスセンタ102が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0074】A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器1601およびAV機器1602～1604において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。このように、セキュアコンテナ104内にA/V伸長用ソフトウェアSoftを格納することで、SAM1051～1054においてセキュアコンテナ104内に格納されたA/V伸長用ソフトウェアSoftを用いてコンテンツデータCの伸長を行うことができ、コンテンツデータC毎あるいはコンテンツプロバイ

をコンテンツプロバイダ101が自由に設定しても、ユーザに多大な負担をかけることはない。

【0075】また、コンテンツファイルCFには、図4に示すように、ファイルリーダと、秘密鍵データK_{op,s}によるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、SAM1051～1054において、異系列の複数のセキュアコンテナ104から受信したそれぞれ異なるフォーマットのコンテンツファイルCFを格納した複数のセキュアコンテナ104を効率的に処理できる。

【0076】ここで、ファイルリーダは、コンテンツファイルCFおよびそれに対応するキーファイルKFを読む際に用いられ、これらのファイルの読み込み手順などを示している。但し、本実施形態では、EMDサービスセンタ102からSAM1051～1054に、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ104のコンテンツファイルCFは、ファイルリーダを格納していない。

【0077】本実施形態では、コンテンツデータCの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータCを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータCがセキュアコンテナ104内に格納されている。すなわち、これらの事項をコンテンツプロバイダ101が自由に決定できる。

【0078】＜キーファイルKF＞図5は、図3(A)に示すキーファイルKFを詳細に説明するための図である。本実施形態では、例えば、図6に示すように、コンテンツプロバイダ101からEMDサービスセンタ102に登録用モジュールMod2が送られて登録処理が行われた後に、例えば6カ月分のキーファイルKFがEMDサービスセンタ102からコンテンツプロバイダ101に送られ、キーファイルデータベースに格納される。このとき、登録用モジュールMod2およびキーファイルKFの送受信時に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証およびセッション鍵データK_{ses}による暗号化および復号が行われる。キーファイルKFは、コンテンツデータC毎に存在し、後述するように、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSDによって、対応するコンテンツファイルCFとの間でリンク関係が指定されている。キーファイルKFには、図3(B)および図5に示すように、ヘッダ、コンテンツ鍵データK_c、権利書データ（使用許諾条件）106、SAMプログラム・ダウンロード・コンテナSDC1～SDC3および署名データSIG_{KI,ESC}が格納されている。ここで、コンテンツプロバイダ101の秘密鍵データK_{ESC,s}を用いた

署名データは、図3(B)に示すようにキーファイルKFに格納される全てのデータに対しての署名データK1.Escにしてもよいし、図5に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データKcおよび権利書データ106に対しての署名データと、SAMプログラム・ダウンロード・コンテナSDCに対しての署名データとを別々に設けてもよい。コンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC1～SDC3とは、それぞれ対応する期間のライセンス鍵データKD1～KD6を用いて暗号化されている。なお、権利書データ106は、キーファイルKF内に格納しないでもよい。この場合には、例えば、権利書データ106はライセンス鍵データによる暗号化を行わずに、署名データを付加する。

【0079】ヘッダデータには、図5に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データKesc.sによる署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルKFに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ101の秘密鍵データKesc.sによる署名データが含まれる。なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図7に示すような情報を含めてもよい。また、コンテンツIDには、例えば、図8に示す情報が含まれている。コンテンツIDは、EMDサービスセンタ102あるいはコンテンツプロバイダ101において作成され、EMDサービスセンタ102において作成された場合には図8に示すようにEMDサービスセンタ102の秘密鍵データKesc.sによる署名データが添付され、コンテンツプロバイダ101において作成された場合にはコンテンツプロバイダ101の秘密鍵データKcp.sが添付される。コンテンツIDは、コンテンツプロバイダ101およびEMDサービスセンタ102の何れで作成してもよい。

【0080】ディレクトリ構造データは、セキュアコンテナ104内におけるコンテンツファイルCF相互間の対応関係と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。例えば、セキュアコンテナ104内にコンテンツファイルCF1～CF3と、それらに対応するキーファイルKF1～KF3が格納されている場合には、図9に示すように、コンテンツファイルCF1～CF3相互間のリンクと、コンテンツファイルCF1～CF3とキーファイルKF1～KF3との間のリンク関係とがディレクトリ構造データによって確立される。ハイパーリンクデータは、セキュアコンテナ104の内外の全てのファイルを対象として、キーファイルKF相互間での階層構造と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。具体的

には、図10に示すように、セキュアコンテナ104内にコンテンツファイルCFおよびキーファイルKF毎のリンク先のアドレス情報とその認証値(ハッシュ値)とを格納し、ハッシュ関数H(x)を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【0081】また、権利書データ106は、コンテンツデータCの運用ルールを定義した記述子(ディスクリプター)であり、例えば、コンテンツプロバイダ101の運用者が希望する卸売価格やコンテンツデータCの複製ルールなどが記述されている。具体的には、権利書データ106には、図5に示すように、コンテンツID、コンテンツプロバイダ101の識別子CP_ID、権利書データ106の有効期限、EMDサービスセンタ102の通信アドレス、利用空間調査情報、卸売価格情報SRP(Suggested Retailer' Price)、取扱方針、取扱制御情報(Usage Control)、商品デモ(試聴)の取扱制御情報およびそれらについての署名データなどが含まれる。ここで、取扱制御情報は、例えば、再配付(Re-Distribution)、再生課金(Pay Per Use)、完全買い切り(Sell Through)、時間制限買い切り(Time Limited Sell Through)、回数制限買い切り(Shell Through Pay Per Play N)、時間課金(Pay Per Time)、SCMS機器への再生課金、ブロック課金(Pay Per Block)などの購入形態のうち許諾された購入形態を示す情報である。

【0082】なお、後述する第2実施形態のように、サービスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテナ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテナ104を提供するサービスプロバイダ310の識別子SP_IDが含まれる。

【0083】また、SAMプログラム・ダウンロード・コンテナSDC1～SDC3には、図5に示すように、SAM1051～1054内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス(文法)を示すUCP-L(Label)、R(Reader)などのラベルリーダと、SAM1051～1054に内蔵された記憶部192(マスクROM1104、不揮発性メモリ1105などのフラッシュROM)の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。SAM1051～1054のマスクROM1104および不揮発性メモリ1105では、ロック鍵データに基づいて、記憶データの書き換えおよび消去を許可するか否かをブロック単位で制御する。

【0084】以下、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を供給する形態について説明する。コンテンツプロバ

イダ101は、前述したように、セキュアコンテナ104を、オフラインおよび/またはオンラインでユーザホームネットワーク103に供給する。コンテンツプロバイダ101は、オンラインで、セキュアコンテナ104をユーザホームネットワーク103のネットワーク機器1601に供給する場合には、ネットワーク機器1601との間で相互認証を行ってセッション鍵(共通鍵)データKsesを共有し、セキュアコンテナ104を当該セッション鍵データKsesを用いて暗号化してEMDサービスセンタ102に送信する。セッション鍵データKsesは、相互認証を行う度に新たに生成される。このとき、セキュアコンテナ104を送信する通信プロトコルとして、デジタル放送であればMHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルを用い、インターネットであればXML/SMIL/HTML(Hyper TextMarkup Language)を用い、これらの通信プロトコル内に、セキュアコンテナ104を、符号化方式に依存しない形式でトンネリングして埋め込む。従って、通信プロトコルとセキュアコンテナ104との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ104のフォーマットを柔軟に設定できる。なお、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。本実施形態では、コンテンツプロバイダ101、EMDサービスセンタ102およびネットワーク機器1601に内蔵された相互間で通信を行うためのモジュールとして、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0085】また、コンテンツプロバイダ101は、オフラインで、セキュアコンテナ104をユーザホームネットワーク103に供給する場合には、以下に示すようなROM型あるいはRAM型の記録媒体にセキュアコンテナ104を記録して、当該記録媒体を所定の流通経路を経てユーザホームネットワーク103に供給する。図11は、本実施形態で用いられるROM型の記録媒体1301を説明するための図である。図11に示すように、ROM型の記録媒体1301は、ROM領域131、セキュアRAM領域132およびメディアSAM133を有する。ROM領域131には、図3(A)に示したコンテンツファイルCFが記憶されている。また、セキュアRAM領域132は、記憶データに対してのアクセスに所定の許可(認証)が必要な領域であり、図3(B)、(C)に示したキーファイルKFおよび公開鍵証明書データCERcpと機器の種類に応じて固有の値を持つ記録用鍵データKstrとを引数としてMAC(Message Authentication Code)関数を用いて生成した署名データと、当該キーファイルKFおよび公開鍵証明書デー

タCERcpとを記録媒体に固有の値を持つメディア鍵データKmedを用いて暗号化したデータとが記憶される。また、セキュアRAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM1051~1055を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。本実施形態で用いられるメディアSAMおよび後述するメディア・ドロブSAM260では、これら相互間で通信を行う際に、自らが持つリボケーションリストと相手方が持つリボケーションリストとの作成時を比較し、自らが持つリボケーションリストの作成時が前の場合には、相手方が持つリボケーションリストによって自らのリボケーションリストを更新する。また、セキュアRAM領域132には、後述するようにユーザホームネットワーク103のSAM1051~1054においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御データ166がセキュアRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体1301となる。メディアSAM133には、例えば、ROM型の記録媒体1301の識別子であるメディアIDと、メディア鍵データKmedとが記憶されている。メディアSAM133は、例えば、相互認証機能を有している。

【0086】本実施形態で用いるROM型の記録媒体としては、例えば、図11に示すものの他に、図12に示すROM型の記録媒体1302および図13に示すROM型の記録媒体1303なども考えられる。図12に示すROM型の記録媒体1302は、ROM領域131と認証機能を有するメディアSAM133とを有し、図11に示すROM型の記録媒体1301のようにセキュアRAM領域132を備えていない。ROM型の記録媒体1302を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図13に示すROM型の記録媒体1303は、ROM領域131およびセキュアRAM領域132を有し、図11に示すROM型の記録媒体1301のようにメディアSAM133を有していない。ROM型の記録媒体1303を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、ROM型の記録媒体1303を用いる場合には、SAMとの間で相互認証は行わない。また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いられる。

【0087】本実施形態で用いるRAM型の記録媒体としては、例えば図14に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRAM領域134を有するRAM型の記録媒体1304がある。RAM型の記録媒体1304では、メディアS

AM133は認証機能を持ち、キーファイルKFを記憶する。また、RAM領域134には、コンテンツファイルCFが記録される。また、本実施形態で用いるRAM型の記録媒体としては、その他に、図15に示すRAM型の記録媒体1305および図16に示すRAM型の記録媒体1306なども考えられる。図15に示すRAM型の記録媒体1305は、セキュアでないRAM領域134と認証機能を有するメディアSAM133とを有し、図14に示すRAM型の記録媒体1304のようにセキュアRAM領域132を備えていない。RAM型の記録媒体1305を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図16に示すRAM型の記録媒体1306は、セキュアRAM領域132およびセキュアでないRAM領域134を有し、図14に示すRAM型の記録媒体1304のようにメディアSAM133を有していない。RAM型の記録媒体1306を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、RAM型の記録媒体1306を用いる場合には、SAMとの間で相互認証は行わない。

【0088】ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体1301を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM1051~1054では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0089】また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データKcとを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データKcを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データKcはライセンス鍵データKD1~KD6で暗号化されているが、ライセンス鍵データKD1~KD6は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM1051~1055に事前に(SAM1051~1054がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータC

の利用が可能になる。なお、本発明は、後述するようにコンテンツデータCとコンテンツ鍵データKcとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0090】以下、コンテンツプロバイダ101におけるセキュアコンテナ104の作成に係わる処理の流れを説明する。図17、図18、図19は、当該処理の流れを説明するためのフローチャートである。

10 ステップS17-1: コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。また、コンテンツプロバイダ101は、予め自らの公開鍵証明書データCERcpをEMDサービスセンタ102から得ている。

20 ステップS17-2: コンテンツプロバイダ101は、新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツIDを割り振り、コンテンツマスタソースデータベースに格納して一元的に管理する。

ステップS17-3: コンテンツプロバイダ101は、ステップS17-2において一元的に管理した各々のコンテンツマスタソースにメタデータMetaを作成し、これをメタデータデータベースに格納して管理する。

30 【0091】ステップS17-4: コンテンツプロバイダ101は、コンテンツマスタソースデータベースからコンテンツマスタソースであるコンテンツデータを読み出して電子透かし情報を埋め込む。

ステップS17-5: コンテンツプロバイダ101は、ステップS17-4で埋め込んだ電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップS17-6: 電子透かし情報が埋め込まれたコンテンツデータを圧縮する。

ステップS17-7: コンテンツプロバイダ101は、ステップS17-6で圧縮したコンテンツデータを伸長してコンテンツデータを生成する。

40 ステップS17-8: コンテンツプロバイダ101は、伸長したコンテンツデータの聴覚検査を行う。

ステップS17-9: コンテンツプロバイダ101は、コンテンツデータに埋め込まれた電子透かし情報を、ステップS17-5でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。そして、コンテンツプロバイダ101は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップS17-10の処理を行い、何れか一方が失敗した場合にはステップS17-4の処理を繰り返す。

50 【0092】ステップS17-10: コンテンツプロバイダ101は、乱数を発生してコンテンツ鍵データKc

を生成し、これを保持する。また、コンテンツプロバイダ101は、ステップS17-6で圧縮したコンテンツデータを、コンテンツ鍵データKcを用いて暗号化する。

【0093】ステップS17-11：コンテンツプロバイダ101は、図4(A)に示すコンテンツファイルCFを作成し、これをコンテンツファイルデータベースに格納する。

【0094】ステップS17-12：コンテンツプロバイダ101は、コンテンツデータCについての権利書データ106を作成する。

ステップS17-13：コンテンツプロバイダ101は、SRPを決定する。

ステップS17-14：コンテンツプロバイダ101は、コンテンツID、コンテンツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力する。

ステップS17-15：コンテンツプロバイダ101は、ライセンス鍵データKD₁～KD₃で暗号化されたキーファイルKFをEMDサービスセンタ102から入

力する。
ステップS17-16：コンテンツプロバイダ101は、入力したキーファイルKFをキーファイルデータベースに格納する。

【0095】ステップS17-17：コンテンツプロバイダ101は、コンテンツファイルCFとキーファイルKFとのリンク関係をハイパーリンクで結ぶ。

ステップS17-18：コンテンツプロバイダ101は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データKcp,sを用いて署名データSIG_{6,CP}を生成する。また、コンテンツプロバイダ101は、キーファイルKFのハッシュ値をとり、秘密鍵データKcp,sを用いて署名データSIG_{7,CP}を生成する。

【0096】ステップS17-19：コンテンツプロバイダ101は、図4に示すように、コンテンツファイルCF、キーファイルKF、公開鍵証明書データCERcp、署名データSIG_{6,CP}、SIG_{7,CP}、SIG_{1,ESC}を格納したセキュアコンテナ104を作成する。

【0097】ステップS17-20：複数のセキュアコンテナを用いたコンボジット形式でコンテンツデータを提供する場合には、ステップS17-1～B19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキーファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク関係をハイパーリンクなどを用いて結ぶ。

ステップS17-21：コンテンツプロバイダ101は、作成したセキュアコンテナ104をセキュアコンテナデータベースに格納する。

【0098】[EMDサービスセンタ102] 図20は、EMDサービスセンタ102の主な機能を示す図で

ある。EMDサービスセンタ102は、主に、図20に示すように、ライセンス鍵データをコンテンツプロバイダ101およびSAM105₁～105₄に供給する処理と、公開鍵証明書データCERcp、CER_{SAM1}～CER_{SAM4}の発行処理と、キーファイルKFの発行処理、利用履歴データ108に基づいた決済処理(利益分配処理)とを行う。

【0099】<ライセンス鍵データの供給処理> 先ず、EMDサービスセンタ102からユーザホームネットワーク103内のSAM105₁～105₄にライセンス鍵データを送信する際の処理の流れを説明する。EMDサービスセンタ102では、所定期間毎に、例えば、3カ月分のライセンス鍵データKD₁～KD₃を鍵データベースから読み出して、各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKesc,sを用いて、それぞれに対応する署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}を作成する。そして、EMDサービスセンタ102は、3カ月分のライセンス鍵データKD₁～KD₃およびそれらの署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}を、SAM105₁～105₄と間の相互認証で得られたセッション鍵データKsesを用いて暗号化した後に、SAM105₁～105₄に送信する。また、同様に、EMDサービスセンタ102は、コンテンツプロバイダ101に、例えば、6カ月分のライセンス鍵データKD₁～KD₆を送信する。

【0100】<公開鍵証明書データの発行処理> 次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データCERcpの発行要求を受けた場合の処理を説明する。EMDサービスセンタ102は、コンテンツプロバイダ101の識別子CP_ID、公開鍵データKcp,pおよび署名データSIG_{9,CP}をコンテンツプロバイダ101から受信すると、これらを、コンテンツプロバイダ101との間の相互認証で得られたセッション鍵データKsesを用いて復号する。そして、当該復号した署名データSIG_{9,CP}の正当性を検証した後に、識別子CP_IDおよび公開鍵データKcp,pに基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がCPデータベースに登録されているか否かを確認する。そして、EMDサービスセンタ102は、当該コンテンツプロバイダ101のX.509形式の公開鍵証明書データCERcpを証明書データベースから読み出し、公開鍵証明書データCERcpのハッシュ値をとり、EMDサービスセンタ102の秘密鍵データKesc,sを用いて、署名データSIG_{1,ESC}を作成する。そして、EMDサービスセンタ102は、公開鍵証明書データCERcpおよびその署名データSIG_{1,ESC}を、コンテンツプロバイダ101との間の相互認証で得られたセッション鍵データKsesを用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0101】なお、EMDサービスセンタ102がSAM1051から、公開鍵証明書データCERSAM1の発行要求を受けた場合の処理も、SAM1051との間で処理が行われる点を除いて、公開鍵証明書データCERCPの発行要求を受けた場合の処理と同じである。公開鍵証明書データCERCPも、X.509形式で記述されている。なお、本発明では、EMDサービスセンタ102は、例えば、SAM1051の出荷時に、SAM1051の秘密鍵データK_{SAM1,s}および公開鍵データK_{SAM1,p}をSAM1051の記憶部に記憶する場合には、当該出荷時に、公開鍵データK_{SAM1,p}の公開鍵証明書データCERSAM1を作成してもよい。このとき、当該出荷時に、公開鍵証明書データCERSAM1を、SAM1051の記憶部に記憶してもよい。

【0102】＜キーファイルKFの発行処理＞EMDサービスセンタ102は、コンテンツプロバイダ101から図6に示す登録用モジュールMod2を受信すると、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK_{SES}を用いて登録用モジュールMod2を復号する。そして、EMDサービスセンタ102は、鍵データベースから読み出した公開鍵データK_{CP,p}を用いて、署名データSIG_{MI,CP}の正当性を検証する。次に、EMDサービスセンタ102は、登録用モジュールMod2に格納された権利書データ106、コンテンツ鍵データK_c、電子透かし情報管理データWMおよびSRPを、権利書データベースに登録する。

【0103】次に、EMDサービスセンタ102は、鍵サーバから読み出した対応する期間のライセンス鍵データKD₁～KD₆を用いて、コンテンツ鍵データK_cおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃とを暗号化する。次に、EMDサービスセンタ102は、ヘッダデータと、コンテンツ鍵データK_cおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃との全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC,s}を用いて署名データSIG_{K1,ESC}を作成する。次に、EMDサービスセンタ102は、図4(B)に示すキーファイルKFを作成し、これをKFデータベースに格納する。次に、EMDサービスセンタ102は、KFデータベースにアクセスを行って得たキーファイルKFを、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0104】＜決算処理＞次に、EMDサービスセンタ102において行なう決済処理について説明する。EMDサービスセンタ102は、ユーザホームネットワーク103の例えばSAM1051から利用履歴データ108およびその署名データSIG_{200,SAM1}を入力すると、利用履歴データ108および署名データSIG_{200,SAM1}

を、SAM1051との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM1051の公開鍵データK_{SAM1}による署名データSIG_{200,SAM1}の検証を行う。

【0105】図21は、利用履歴データ108に記述されるデータを説明するための図である。図21に示すように、利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCに対してEMDサービスセンタ102によってグローバルユニークに付された識別子であるESC__コンテンツID、当該コンテンツデータCに対してコンテンツプロバイダ101によって付された識別子であるCP__コンテンツID、セキュアコンテナ104の配給を受けたユーザの識別子であるユーザID、当該ユーザのユーザ情報、セキュアコンテナ104の配給を受けたSAM1051～1054の識別子SAM__ID、当該SAMが属するホームネットワークグループの識別子であるHNG__ID、ディスカウント情報、トレーシング情報、プライスタグ、当該コンテンツデータを提供したコンテンツプロバイダ101の識別子CP__ID、紹介業者（ポータル:Portal)ID、ハードウェア提供者ID、セキュアコンテナ104を記録した記録媒体の識別子Media__ID、セキュアコンテナ104の提供に用いられた例えば圧縮方法などの所定のコンポーネントの識別子であるコンポーネントID、セキュアコンテナ104のライセンス所有者の識別子LH__ID、セキュアコンテナ104についての決済処理を行うEMDサービスセンタ102の識別子ESC__IDなどが記述されている。なお、後述する第2実施形態では、利用履歴データ308には、上述した利用履歴データ108に記述されたデータに加えて、当該コンテンツデータCに対してサービスプロバイダ310によって付された識別子であるSP__コンテンツIDと、当該コンテンツデータCを配給したサービスプロバイダ310の識別子SP__IDとが記述されている。

【0106】EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

【0107】次に、EMDサービスセンタ102は、利用履歴データ108と、権利書データベースから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。ここで、決済請求権データ152は、当該

データに基づいて、決済機関 91 に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

【0108】次に、EMDサービスセンタ 102 は、決済請求権データ 152 およびその署名データ SIG 99 を、相互認証およびセッション鍵データ Kses による復号を行なった後に、図 1 に示すペイメントゲートウェイ 90 を介して決済機関 91 に送信する。これにより、決済請求権データ 152 に示される金額の金銭が、コンテンツプロバイダ 101 に支払われる。また、EMDサービスセンタ 102 は、決済レポートデータ 107 をコンテンツプロバイダ 101 に送信する。

【0109】【ユーザホームネットワーク 103】ユーザホームネットワーク 103 は、図 1 に示すように、ネットワーク機器 160₁ および A/V 機器 160₂ ~ 160₄ を有している。ネットワーク機器 160₁ は、SAM105₁ を内蔵している。また、AV 機器 160₂ ~ 160₄ は、それぞれ SAM105₂ ~ 105₄ を内蔵している。SAM105₁ ~ 105₄ の相互間は、例えば、IEEE1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。なお、AV 機器 160₂ ~ 160₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 160₁ のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク 103 は、ネットワーク機能を有していない AV 機器のみを有していてもよい。

【0110】以下、ネットワーク機器 160₁ について説明する。図 22 は、ネットワーク機器 160₁ の構成図である。図 22 に示すように、ネットワーク機器 160₁ は、SAM105₁、通信モジュール 162、AV 圧縮・伸長用 SAM163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

【0111】SAM105₁ ~ 105₄ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMD サービスセンタ 102 との間で通信を行う。SAM105₁ ~ 105₄ は、例えば、EMD サービスセンタ 102 によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁ ~ 105₄ の IC (Integrated Circuit) の内部の仕様を知ることはできず、EMD サービスセンタ 102 が当該 IC のインタフェースなどを統一化し、それに従ってネットワーク機器 160₁ および AV 機器 160₂ ~ 160₄ に搭載される。

【0112】SAM105₁ ~ 105₄ は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から

監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ (Tamper Resistance) 性を持ったハードウェアモジュール (IC モジュールなど)、あるいは CPU においてソフトウェア (秘密プログラム) を実行して実現される機能モジュールである。SAM105₁ ~ 105₄ の機能を IC という形で実現する場合は、IC 内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAM を IC という物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分を SAM として定義してもよい。

【0113】以下、SAM105₁ の機能について詳細に説明する。なお、SAM105₂ ~ 105₄ は、SAM105₁ と基本的に同じ機能を有している。図 23 は、SAM105₁ の機能の構成図である。なお、図 23 には、コンテンツプロバイダ 101 からのセキュアコンテンツ 104 を入力し、セキュアコンテンツ 104 内のキーファイル KF を復号する処理に関連するデータの流れが示されている。図 23 に示すように、SAM105₁ は、相互認証部 170、暗号化・復号部 171、172、173、コンテンツプロバイダ管理部 180、ダウンロードメモリ管理部 182、AV 圧縮・伸長用 SAM 管理部 184、EMD サービスセンタ管理部 185、利用監視部 186、課金処理部 187、署名処理部 189、SAM 管理部 190、メディア SAM 管理部 197、作業用メモリ 200 および外部メモリ管理部 811 を有する。ここで、コンテンツプロバイダ管理部 180 およびダウンロードメモリ管理部 182 が本発明の入力処理手段に対応し、課金処理部 187 が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部 172 が本発明の復号手段に対応し、利用監視部 186 が本発明の利用制御手段に対応している。また、暗号化・復号部 173 が請求項 3 等の暗号化手段に対応している。また、後述する例えば図 38 に示すメディア・ドライブ SAM 管理部 855 が本発明の請求項 5 等の記録制御手段に対応している。また、署名処理部 189 が請求項 9 等の署名処理手段に対応している。

【0114】なお、図 23 に示す SAM105₁ の各機能は、前述したように、CPU において秘密プログラムを実行して実現されるか、あるいは所定のハードウェアによって実現される。また、外部メモリ 201 には、以下に示す処理を経て、図 24 に示すように、利用履歴データ 108 および SAM 登録リストが記憶される。ここで、外部メモリ 201 のメモリ空間は、SAM105₁ の外部 (例えば、図示しないホスト CPU) からは見ることはできず、SAM105₁ のみが外部メモリ 201 の記憶領域に対してのアクセスを管理できる。外部メモリ 201 としては、例えば、フラッシュメモリあるいは

強誘電体メモリ (FeRAM) などが用いられる。また、作業用メモリ200としては、例えばSRAMが用いられ、図25に示すように、セキュアコンテナ104、コンテンツ鍵データKc、権利書データ(UCP)106、記憶部192のロック鍵データKLoc、コンテンツプロバイダ101の公開鍵証明書CERcp、利用制御データ(UCS)166、およびSAMプログラム・ダウンロード・コンテナSDC1~SDC3などが記憶される。

【0115】以下、SAM1051の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図23を参照しながら説明する。

【0116】相互認証部170は、SAM1051がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ(共有鍵)Ksesを生成し、これを暗号化・復号部171に出力する。セッション鍵データKsesは、相互認証を行度ごとに新たに生成される。

【0117】暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データKsesを用いて暗号化・復号する。

【0118】ダウンロードメモリ管理部182は、図22に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、相互認証によって得られたセッション鍵データKsesを用いて暗号化して図22に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図26に示すように、HDD(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図23に示す作業用メモリ200あるいは図22に示す外部メモリ201にダウンロードする。キーファイルKFを外部メモリ201に記憶する場合には、例えば、SAM1051において、キーファイルKFをCBCモードでMAC鍵データKNACを用いて暗号化して外部メモリ201に記憶し、最後の暗号文ブロックの一部をMAC(Message Authentication Code)値としSAM1051内に記憶する。そして、外部メモリ201からSAM1051にキーファイルKFを読み出す場合には、SAM1051内で当該読み出したキーファイルKFをMAC鍵データKNACを用いて

復号し、それによって得たMAC値と、既に記憶しているMAC値とを比較することで、キーファイルKFが改竄されているか否かを検証する。この場合に、MAC値ではなく、ハッシュ値を用いてもよい。

【0119】暗号化・復号部172は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1~SDC3を、記憶部192から読み出した対応する期間のライセンス鍵データKD1~KD3を用いて復号する。当該復号されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1~SDC3は、作業用メモリ200に書き込まれる。

【0120】EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0121】署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データKesc.pおよびコンテンツプロバイダ101の公開鍵データKcp.pを用いて、セキュアコンテナ104内の署名データの検証を行なう。

【0122】記憶部192は、SAM1051の外部から読み出しおよび書き換えできない秘密データとして、図27に示すように、有効期限付きの複数のライセンス鍵データKD1~KD3、SAM_ID、ユーザID、パスワード、当該SAMが属するホームネットワークグループの識別子HNG_ID、情報参照ID、SAM登録リスト、機器および記録媒体のリケーションリスト、記録用鍵データKstr、ルートCAの公開鍵データKrcap、EMDサービスセンタ102の公開鍵データKesc.p、EMDサービスセンタ102の公開鍵データKesc.p、ドライブ用SAMの認証用元鍵(共通鍵暗号化方式を採用した場合)、ドライブ用SAの公開鍵証明書(秘密鍵暗号化方式を採用した場合)、SAM1051の秘密鍵データKsam.s(共通鍵暗号化方式を採用した場合)、SAM1051の公開鍵データKsam.pを格納した公開鍵証明書CERsam(秘密鍵暗号化方式を採用した場合)、EMDサービスセンタ102の秘密鍵データKesc.sを用いた公開鍵証明書CERescの署名データSIG22、AV圧縮・伸長用SAM163との間の相互認証用の元鍵データ(共通鍵暗号化方式を採用した場合)、メディアSAMとの間の相互認証用の元鍵データ(共通鍵暗号化方式を採用した場合)、メディアSAMの公開鍵証明書データCERmedsam(公開鍵暗号化方式を採用した場合)、扱える信号の諸元、圧縮方式、接続するモニタ表示能力、フォーマット変換機能、ビットストリームレコーダの有無、権利処理(利益分配)用データ、利益分配する関連エンティティのIDなどを記憶している。なお、図27において、左側に「*」を付し

たデータは、SAM1051の出荷時に記憶部192に記憶されており、それ以外のデータは出荷後に行われるユーザ登録時に記憶部192に記憶される。

【0123】また、記憶部192には、図23に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。記憶部192としては、例えば、フラッシュEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0124】<ライセンス鍵データの受信時の処理>以下、EMDサービスセンタ102から受信したライセンス鍵データKD₁～KD₃を記憶部192に格納する際のSAM1051内での処理の流れを図26および図28を参照しながら説明する。図28は、EMDサービスセンタ102から受信したライセンス鍵データKD₁～KD₃を記憶部192に格納する際のSAM1051内での処理の流れを示すフローチャートである。

ステップS28-1: SAM1051の相互認証部170と、EMDサービスセンタ102との間で相互認証を行なう。

ステップS28-2: ステップS28-1の相互認証によって得られたセッション鍵データK_{SES}で暗号化した3カ月分のライセンス鍵データKD₁～KD₃およびその署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}を、EMDサービスセンタ102からEMDサービスセンタ管理部185を介して作業用メモリ200に書き込む。

【0125】ステップS28-3: 暗号化・復号部171は、セッション鍵データK_{SES}を用いて、ライセンス鍵データKD₁～KD₃およびその署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}を復号する。

ステップS28-4: 署名処理部189は、作業用メモリ200に記憶された署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}の正当性を確認した後に、ライセンス鍵データKD₁～KD₃を記憶部192に書き込む。

【0126】<セキュアコンテナ104をコンテンツプロバイダ101から入力した時の処理>以下、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM1051内での処理の流れを図23および図29を参照しながら説明する。なお、以下に示す例では、SAM1051において、セキュアコンテナ104を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ104の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップS29-1: 図23に示すSAM1051の相互認証部170とコンテンツプロバイダ101との間で相互認証を行なう。

ステップS29-2: SAM1051の相互認証部170とダウンロードメモリ167のメディアSAM167aとの間で相互認証を行なう。

【0127】ステップS29-3: コンテンツプロバイダ101から受信したセキュアコンテナ104を、ダウンロードメモリ167に書き込む。このとき、ステップS29-2で得られたセッション鍵データを用いて、相互認証部170におけるセキュアコンテナ104の暗号化と、メディアSAM167aにおけるセキュアコンテナ104の復号とを行なう。

ステップS29-4: SAM1051は、ステップS29-1で得られたセッション鍵データを用いて、セキュアコンテナ104の復号を行なう。

【0128】ステップS29-5: 署名処理部189は、図3(C)に示す署名データSIG_{1,ESC}の検証を行なった後に、図3(C)に示す公開鍵証明書データCERT_{CP}内に格納されたコンテンツプロバイダ101の公開鍵データK_{CP}を用いて、署名データSIG_{6,CP}, SIG_{7,CP}の正当性を検証する。このとき、署名データSIG_{6,CP}が正当であると検証されたときに、コンテンツファイルCFの作成者および送信者の正当性が確認される。また、署名データSIG_{7,CP}が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0129】ステップS29-6: 署名処理部189は、記憶部192から読み出した公開鍵データK_{ESC,CP}を用いて、図3(B)に示すキーファイルKF内の署名データSIG_{K1,ESC}の正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

【0130】ステップS29-7: 暗号化・復号部172は、記憶部192から読み出した対応する期間のライセンス鍵データKD₁～KD₃を用いて、図3(B)に示すキーファイルKF内のコンテンツ鍵データK_C、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を復号し、これらを作業用メモリ200に書き込む。

【0131】以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図30を参照しながら説明する。

【0132】利用監視部186は、作業用メモリ200から権利書データ106および利用制御データ166を読み出し、当該読み出した権利書データ106および利用制御データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ106は、図29を用いて説明したように、復号後に作業用メモリ200に記憶されたキーファイルKF内に格納されている。また、利用制御データ166は、後述するように、ユーザによって購入形態が決定されたときに、作業用メモリ200に記憶される。なお、利用制御データ166には、当該コンテンツデータ

Cを購入したユーザのユーザIDおよびトレーシング(Tracing)情報が記述され、取扱制御情報として購入形態決定処理で決定された購入形態が記述されている点を除いて、図3に示す権利書データ106と同じデータが記述されている。

【0133】課金処理部187は、図23に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0134】また、課金処理部187は、必要に応じて、作業用メモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。ここで、販売価格および標準小売価格データSRPは、復号後に作業用メモリ200に記憶された図3(B)に示すキーファイルKFの権利書データ106内に格納されている。課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0135】また、課金処理部187は、操作信号S165に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御(UCS: Usage Control Status)データ166を生成し、これを作業用メモリ200に書き込む。本実施形態では、購入形態を決定した後に、利用制御データ166を作業用メモリ200に記憶する場合を例示したが、利用制御データ166およびコンテンツ鍵データKcを外付けメモリである外部メモリ201に格納するようにしてもよい。外部メモリ201としては、前述したように、例えばNVRAMであるフラッシュメモリが用いられる。外部メモリ201に書き込みを行う場合には外部メモリ201の正当性の検証であるインテグリティチェック(Integrity Check)を行うが、この際に外部メモリ201の記憶領域を複数のブロックに分け、ブロック毎にSHA-1あるいはMACなどでハッシュ値を求め、当該ハッシュ値をSAM1051内で管理する。なお、SAM1051において、購入形態を決定せずに、セキュアコンテナ104を他のSAM1052~1054に転送してもよい。この場合には、利用制御データ166は作成されない。

【0136】コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切り(Sell Through)、利用期間に制限を持たせるタイムリミテッド(Time Limited)、再生する度に課金を行なう再生課金(Pay Per Play)、SCMS機器を用いた複製において再生する度に課金を行なう再生

課金(Pay Per SCMS)、SCMS機器において複製を認める(Sell Through SCMSCopy)、および複製のガードを行わずに再生する度に課金を行う再生課金(Pay Per Copy N without copy guard)などがある。ここで、利用制御データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0137】なお、決定された購入形態が再生課金である場合には、例えば、SAM1051からコンテンツプロバイダ101に利用制御データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM1051に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0138】EMDサービスセンタ管理部185は、所定の期間毎に、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データK_{SAM1}を用いて利用履歴データ108の署名データSIG_{200, SAM1}を作成し、署名データSIG_{200, SAM1}を利用履歴データ108と共にEMDサービスセンタ102に送信する。EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0139】ダウンロードメモリ管理部182は、例えば、図22に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、作業用メモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196をAV圧縮・伸長用SAM管理部184に出力する。また、AV圧縮・伸長用SAM管理部184は、図22に示す購入形態決定操作部165からの操作信号S165に応じてコン

テンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びに作業用メモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199をAV圧縮・伸長用SAM管理部184に出力する。

【0140】ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。AV圧縮・伸長用SAM163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、AV圧縮・伸長用SAM163がデータ(信号)を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0141】<ダウンロードしたセキュアコンテンツの購入形態決定処理>以下、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテンツ104の購入形態を決定するまでの処理の流れを図30および図31を参照しながら説明する。なお、以下に示す処理では、セキュアコンテンツ104の購入形態を決定する際に、セキュアコンテンツ104内の各データの署名データの検証を行わない(前述したようにセキュアコンテンツ104の受信時に署名データの検証を行う)場合を例示するが、当該購入形態を決定する際にこれらの署名データの検証を行ってもよい。図31は、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテンツ104の購入形態を決定するまでの処理の流れを示すフローチャートである。

ステップS31-1: ユーザによる図22に示す購入・利用形態決定操作部165の操作に応じた試聴モードを示す操作信号S165が課金処理部187に出力されたか否かを判断し、出力されたと判断した場合にはステップS31-2の処理を実行し、出力されていないと判断した場合にはステップS31-5の処理を実行する。

【0142】ステップS31-2: 作業用メモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図22に示すAV圧縮・伸長用SAM163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データKsesによる暗号化および復号が行なわれる。

【0143】ステップS31-3: ユーザによる図22に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部1

87に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、AV圧縮・伸長用SAM管理部184を介して、図22に示すAV圧縮・伸長用SAM163に出力される。このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKsesによる暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データKsesによる暗号化・復号とが行なわれる。コンテンツファイルCFは、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データKsesを用いて復号された後に、復号部222に出力される。

【0144】ステップS31-4: 復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。次に、電子透かし情報処理部224においてコンテンツデータCにユーザ電子透かし情報用データ196が埋め込まれ、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。また、電子透かし情報処理部224では、コンテンツデータCに埋め込まれている電子透かし情報が検出され、当該検出の結果に基づいて、処理の停止の有無を決定する。

【0145】ステップS31-5: ユーザが購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

ステップS31-6: 課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御データ166が作業用メモリ200に書き込まれる。以後は、利用監視部186において、利用制御データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御(監視)される。

【0146】ステップS31-7: 後述する図32

(C)に示す新たなキーファイルKF1が作成され、当該作成されたキーファイルKF1がダウンロードメモリ管理部182を介してダウンロードメモリ167あるいはその他のメモリに記憶される。図32(C)に示すように、キーファイルKF1に格納された利用制御データ166はストレージ鍵データKstrおよびメディア鍵データKmedを用いてDESのCBCモードを利用して順に暗号化されている。ここで、記録用鍵データK

STR は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データK_{MD} は、記録媒体にユニークなデータである。

【0147】ステップS31-8:署名処理部189において、SAM1051の秘密鍵データK_{SAM1}を用いて、キーファイルKF1のハッシュ値H_{K1}が作成され、当該作成されたハッシュ値H_{K1}が、キーファイルKF1と対応付けられて作業用メモリ200に書き込まれる。ハッシュ値H_{K1}は、キーファイルKF1の作成者の正当性およびキーファイルKF1が改竄されたか否かを検証するために用いられる。なお、購入形態が決定されたコンテンツデータCを、例えば、記録媒体に記録したり、オンラインを介して送信する場合には、図32に示すように、キーファイルKF1およびハッシュ値H_{K1}、コンテンツファイルCFおよびその署名データSIG₆.CP、キーファイルKFおよびその署名データSIG₇.CP、公開鍵証明書データCER_{CP}およびその署名データSIG₁.ESC、公開鍵証明書データCER_{SAM1}およびその署名データSIG₂.ESCを格納したセキュアコンテナ104pが作成される。上述したようにセキュアコンテナ104の購入形態を決定すると、利用制御データ166が生成されて作業用メモリ200に記憶されるが、SAM1051において再び同じセキュアコンテナ104について購入形態を再決定する場合には、操作信号S165に応じて作業用メモリ200に記憶されている利用制御データ166が更新される。

【0148】<コンテンツデータの再生処理>次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図33を参照しながら説明する。図33は、当該処理を示すフローチャートである。当該処理を行う前提として、前述した購入形態の決定処理によって作業用メモリ200に、利用制御データ166が格納されている。

ステップS33-1:作業用メモリ200から利用監視部186に、利用制御データ166が読み出され、利用制御データ166が示す再生条件が解釈・検証され、その結果に基づいて以後の再生処理が行われるように監視される。

ステップS33-2:図30に示す相互認証部170と、図22に示すAV圧縮・伸長用SAM163の相互認証部220との間で相互に認証が行われ、セッション鍵データK_{SES}が共有される。

【0149】ステップS33-3:ステップS33-1で解釈・検証された再生条件と、作業用メモリ200から読み出されたコンテンツ鍵データK_Cとが、ステップS33-2で得られたセッション鍵データK_{SES}を用い

て暗号化された後に、AV圧縮・伸長用SAM163に出力される。これによって、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データK_{SES}を用いて再生条件およびコンテンツ鍵データK_Cが復号される。

【0150】ステップS33-4:ダウンロードメモリ167から読み出されたコンテンツファイルCFが、ステップS33-2で得られたセッション鍵データK_{SES}を用いて暗号化された後に、AV圧縮・伸長用SAM163に出力される。これによって、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データK_{SES}を用いてコンテンツファイルCFが復号される。続いて、AV圧縮・伸長用SAM163の伸長部223において、コンテンツファイルCF内のコンテンツデータCが伸長され、電子透かし情報処理部224においてユーザ電子透かし情報を埋め込んだ後に再生モジュール169において再生される。

【0151】ステップS33-5:必要に応じて、ステップS33-1で読み出された利用制御データ166が更新され、再び作業用メモリ200に書き込まれる。また、外部メモリ201に記憶されている利用履歴データ108も更新される。

【0152】<一の機器の利用制御 態データ(USC)166を使用して他の機器で再購入を行う場合の処理>先ず、図34に示すように、例えば、ネットワーク機器1601のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの購入形態を前述したように決定した後に、当該コンテンツファイルCFを格納した新たなセキュアコンテナ104xを生成し、バス191を介して、AV機器1602のSAM1052にセキュアコンテナ104xを転送するまでのSAM1051内での処理の流れを図35および図36を参照しながら説明する。

【0153】図36は、当該処理のフローチャートである。図36に示す処理を行う前提として、前述した購入処理によって、SAM1051の作業用メモリ200には図32(C)に示すキーファイルKF1およびハッシュ値H_{K1}が記憶されている。

ステップS36-1:ユーザは、購入・利用形態決定操作部165を操作して、購入形態を既に決定したセキュアコンテナをSAM1052に転送することを指示する。課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。

【0154】ステップS36-2:SAM1051は、後述するSAM登録リストを検証し、セキュアコンテナの転送先のSAM1052が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS36-3以降の処理を行う。また、SAM1051は、SAM1052がホームネット

ワーク内のSAMであるか否かの検証も行う。

【0155】ステップS36-3:相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データKsesを共用する。

【0156】ステップS36-4: SAM管理部190は、ダウンロードメモリ211から図32(A)に示すコンテンツファイルCFおよび署名データSIG_{6,CP}を読み出し、これについてのSAM105₁の秘密鍵データK_{SAM1}を用いた署名データSIG_{41,SAM1}を署名処理部189に作成させる。

【0157】ステップS36-5: SAM管理部190は、ダウンロードメモリ211から図32(B)に示すキーファイルKFおよび署名データSIG_{7,CP}を読み出し、これについてのSAM105₁の秘密鍵データK_{SAM1}を用いた署名データSIG_{42,SAM1}を署名処理部189に作成させる。

【0158】ステップS36-6: SAM管理部190は、図37に示すセキュアコンテナ104xを作成する。

ステップS36-7: 暗号化・復号部171において、ステップS36-3で得たセッション鍵データKsesを用いて、図37に示すセキュアコンテナ104xが暗号化される。

【0159】ステップS36-8: SAM管理部190は、セキュアコンテナ104xを図34に示すAV機器160₂のSAM105₂に出力する。このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0160】以下、図34に示すように、SAM105₁から入力した図37に示すセキュアコンテナ104xを、RAM型などの記録媒体(メディア)1304に書き込む際のSAM105₂内での処理の流れを図38、図39および図40を参照して説明する。図39および図40は、当該処理を示すフローチャートである。ここで、RAM型の記録媒体1304は、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

【0161】ステップS39-1: SAM105₂は、SAM登録リストを検証し、セキュアコンテナの転送元のSAM105₁が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS39-2以降の処理を行う。また、SAM105₂は、SAM105₁がホームネットワーク内のSAMであるか否かの検証も行う。

【0162】ステップS39-2: 前述したステップS36-2に対応する処理として、SAM105₂は、SAM105₁との間で相互認証を行って得たセッション鍵データKsesを共用する。

ステップS39-3: SAM105₂のSAM管理部1

90は、図34および図38に示すように、ネットワーク機器160₁のSAM105₁からセキュアコンテナ104xを入力する。

ステップS39-4: 暗号化・復号部171は、ステップS39-2で共用したセッション鍵データKsesを用いて、SAM管理部190を介して入力したセキュアコンテナ104xを復号する。

【0163】ステップS39-5: セッション鍵データKsesを用いて復号されたセキュアコンテナ104x内のコンテンツファイルCFが、図32に示すメディア・ドラブSAM260におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のRAM領域134に記録される。

【0164】ステップS39-6: セッション鍵データKsesを用いて復号されたセキュアコンテナ104x内の署名データSIG_{6,CP}、SIG_{41,SAM1}と、キーファイルKFおよびその署名データSIG_{7,CP}、SIG_{42,SAM1}と、キーファイルKF₁およびそのハッシュ値Hk₁と、公開鍵署名データCER_{CP}およびその署名データSIG_{1,ESC}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22,ESC}とが、作業用メモリ200に書き込まれる。

【0165】ステップS39-7: 署名処理部189において、記憶部192から読み出した公開鍵データK_{CP,P}を用いて、公開鍵証明書データCER_{CP}、CER_{SAM1}の正当性が確認される。そして、署名処理部189において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{CP,P}を用いて、署名データSIG_{6,CP}の正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1,P}を用いて、署名データSIG_{41,SAM1}の正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。

【0166】ステップS39-8: 署名処理部189は、公開鍵データK_{CP}、K_{SAM1,P}を用いて、作業用メモリ200に記憶されている署名データSIG_{7,CP}、SIG_{42,SAM1}の正当性を検証する。そして、署名データSIG_{7,CP}、SIG_{42,SAM1}が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0167】ステップS39-9: 署名処理部189は、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて、図37(B)に示すキーファイルKFに格納された署名データSIG_{K1,ESC}の正当性を確認する。そして、署名データSIG_{K1,ESC}が正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

【0168】ステップS39-10：署名処理部189は、ハッシュ値Hk1の正当性を検証し、キーファイルKF1の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルKF1の作成者と送信元とが同じ場合を述べたが、キーファイルKF1の作成者と送信元とが異なる場合には、キーファイルKF1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0169】ステップS39-11：利用監視部186は、ステップS39-10で復号されたキーファイルKF1に格納された利用制御データ166を用いて、以後のコンテンツデータCの購入・利用形態を制御する。

【0170】ステップS39-12：ユーザは、購入・利用形態決定操作部165を操作して購入形態を決定し、当該操作に応じた操作信号S165が、課金処理部187に出力される。

ステップS39-13：課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。また、課金処理部187は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ166を更新する。

【0171】ステップS39-14：暗号化・復号部173は、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMEDおよび購入者鍵データKPINを順に用いて、ステップS39-12で生成された利用制御データ166を暗号化してメディア・ドライブSAM管理部855に出力する。

ステップS39-15：メディア・ドライブSAM管理部855は、新たな利用制御データ166を格納したキーファイルKF1を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のセキュアRAM領域132に記録する。なお、メディア鍵データKMEDは、図38に示す相互認証部170と図34に示すRAM型の記録媒体1304のメディアSAM133との間の相互認証によって記憶部192に事前に記憶されている。

【0172】ここで、記録用鍵データKSTRは、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類(当該例では、AV機器1602)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データKSTRは、このような場合において、不正コピーを防止する役割を果たす。なお、本実施

形態では、記録用鍵データKSTRを用いた暗号化を行わないようにしてもよい。

【0173】また、メディア鍵データKMEDは、記録媒体(当該例では、RAM型の記録媒体1304)にユニークなデータである。メディア鍵データKMEDは、記録媒体(当該例では、図34に示すRAM型の記録媒体1304)側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データKMEDを用いた暗号化および復号を行うことがセキュリティの観点から好ましい。

このとき、メディア鍵データKMEDは、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内の図示しないホストCPUの管理外の領域に記憶されている。なお、本実施形態のように、機器側のSAM(当該例では、SAM1052)とメディアSAM(当該例では、メディアSAM133)との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データKMEDを機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データKMEDを用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データKSTRおよびメディア鍵データKMEDが、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0174】また、購入者鍵データKPINは、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データKPINは、EMDサービスセンタ102において管理される。

【0175】ステップS39-16：キーファイルKFが作業用メモリ200から読み出され、メディア・ドライブSAM管理部855を介して、図34に示すメディア・ドライブSAM260によってRAM型の記録媒体1304のセキュアRAM領域132に書き込まれる。

【0176】また、上述した実施形態では、メディア・ドライブSAM260による処理を経て、キーファイルKF、KF1をRAM型の記録媒体1304のセキュアRAM領域132に記録する場合を例示したが、図34において点線で示すように、SAM1052からメディアSAM133にキーファイルKF、KF1を記録するようにしてもよい。

【0177】また、上述した実施形態では、SAM1051からSAM1052にセキュアコンテンツ104xを送信する場合を例示したが、ネットワーク機器1601のホストCPUおよびAV機器1602のホストCPUによって、コンテンツファイルCFおよび権利書データ106をネットワーク機器1601からAV機器1602に送信してもよい。この場合には、SAM1051からSAM1052に、利用制御データ166およびコンテンツ鍵データKcが送信される。

【0178】また、その他の実施形態として、例えば、SAM105₁において購入形態を決定し、SAM105₂では購入形態を決定せずに、SAM105₁において生成した利用制御データ166をSAM105₂でそのまま用いてもよい。この場合には、利用履歴データ108は、SAM105₁において生成され、SAM105₂では生成されない。また、コンテンツデータCの購入は、例えば、複数のコンテンツデータCからなるアルバムを購入する形態で行ってもよい。この場合に、アルバムを構成する複数のコンテンツデータCは、異なるコンテンツプロバイダ101によって提供されてもよい（後述する第2実施形態の場合には、さらに異なるサビスプロバイダ310によって提供されてもよい）。また、アルバムを構成する一部のコンテンツデータCについての購入を行った後に、その他のコンテンツデータCを追加する形で購入を行い、最終的にアルバムを構成する全てのコンテンツデータCを購入してもよい。

【0179】図41は、コンテンツデータCの種々の購入形態の例を説明するための図である。図41に示すように、AV機器160₃は、ネットワーク機器160₁がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入し、利用制御データ166aを生成している。また、AV機器160₂は、ネットワーク機器160₁がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入し、利用制御データ166bを生成している。また、AV機器160₃は、AV機器160₂が購入したコンテンツデータCを複製し、AV機器160₂で作成した利用制御データ166bを用いて利用形態を決定している。これにより、AV機器160₃において、利用制御データ166cが作成される。また、AV機器160₃では、利用制御データ166cから利用履歴データ108bが作成される。また、AV機器160₄は、ネットワーク機器160₁がコンテンツプロバイダ101から受信して購入形態を決定したコンテンツデータCを入力し、ネットワーク機器160₁が作成した利用制御データ166を用いて当該コンテンツデータCの購入形態を決定する。これにより、AV機器160₄において、利用制御データ166aが作成される。また、AV機器160₄では、利用制御データ166aから利用履歴データ108aが作成される。なお、利用制御データ166a、166b、166cは、AV機器160₄、160₂、160₃において、それぞれ固有の記録用鍵データS_{STR}、並びに記録メディア（媒体）に固有のメディア鍵データK_{MED}を用いて暗号化され、記録媒体に記録される。本実施形態では、ユーザは、コンテンツデータCの所有権に対して対価を支払うのではなく、使用权に対価を支払う。コンテンツデータの複製は、コンテンツのプロモーションに相当し、マーケットの拡販という観点からコンテンツデータ

の権利者の要請にかなう行為となる。

【0180】＜ROM型の記録媒体のコンテンツデータの購入形態決定処理＞図42に示すように、コンテンツの購入形態が未決定の図11に示すROM型の記録媒体130₁をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器160₂において購入形態を決定する際の処理の流れを図43および図44を参照しながら説明する。図44は、当該処理のフローチャートである。

10 ステップS44-1：AV機器160₂のSAM105₂は、まず、図43に示す相互認証部170と図11に示すROM型の記録媒体130₁のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データK_{MED}を入力する。なお、SAM105₂が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。

【0181】ステップS44-2：ROM型の記録媒体130₁のセキュアRAM領域132に記録されているセキュアコンテンツ104に格納された図3（B）、

20 （C）に示すキーフファイルKFおよびその署名データSIG_{7,CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを、メディア・ドライブSAM管理部855を介して入力して作業用メモリ200に書き込む。

【0182】ステップS44-3：署名処理部189において、署名データSIG_{1,ESC}の正当性を確認した後に、公開鍵証明書データCER_{CP}から公開鍵データK_{CP,P}を取り出し、この公開鍵データK_{CP,P}を用いて、署名データSIG_{7,CP}の正当性、すなわちキーフファイルKFの送信者の正当性を検証する。また、署名処理部189において、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて、キーフファイルKFに格納された署名データSIG_{K1,ESC}の正当性、すなわちキーフファイルKFの作成者の正当性を検証する。

【0183】ステップS44-4：署名処理部189において署名データSIG_{7,CP}、SIG_{K1,ESC}の正当性が確認されると、作業用メモリ200から暗号化・復号部172にキーフファイルKFを読み出す。次に、暗号化・復号部172において、対応する期間のライセンス鍵データKD₁～KD₃を用いて、キーフファイルKFに格納されたコンテンツ鍵データK_c、権利書データ106およびSAMプログラム・ダウンロード・コンテンツSDC₁～SDC₃を復号した後に、作業用メモリ200に書き込む。

【0184】ステップS44-5：図43に示す相互認証部170と図42に示すAV圧縮・伸長用SAM163との間で相互認証を行った後に、SAM105₂のAV圧縮・伸長用SAM管理部184は、作業用メモリ200に記憶されているコンテンツ鍵データK_cおよび権利書データ106に格納された半開示パラメータデータ

199、並びにROM型の記録媒体1301のROM領域131から読み出したコンテンツファイルCFに格納されたコンテンツデータCを図42に示すAV圧縮・伸長用SAM163に出力する。次に、AV圧縮・伸長用SAM163において、コンテンツデータCがコンテンツ鍵データKcを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、AV圧縮・伸長用SAM163からのコンテンツデータCが再生される。

【0185】ステップS44-6：ユーザによる図42に示す購入形態決定操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S165が課金処理部187に入力される。

【0186】ステップS44-7：課金処理部187は、操作信号S165に応じた利用制御データ166を作成し、これを作業用メモリ200に書き込む。

ステップS44-8：作業用メモリ200から暗号化・復号部173に、コンテンツ鍵データKcおよび利用制御データ166が出力される。暗号化・復号部173は、作業用メモリ200から入力したコンテンツ鍵データKcおよび利用制御データ166を、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMDおよび購入者鍵データKPINを用いて順次に暗号化して作業用メモリ200に書き込む。

【0187】ステップS44-9：メディアSAM管理部197において、作業用メモリ200から読み出した、暗号化されたコンテンツ鍵データKcおよび利用制御データ166と、SAMプログラム・ダウンロード・コンテナSDC1～SDC3を用いて図37(C)に示すキーファイルKF1が生成される。また、署名処理部189において、図37(C)に示すキーファイルKF1のハッシュ値Hk1が生成され、当該ハッシュ値Hk1がメディア・ドライブSAM管理部855に出力される。

【0188】ステップS44-10：図43に示す相互認証部170と図42に示すメディアSAM133との間で相互認証を行った後に、メディア・ドライブSAM管理部855は、キーファイルKF1およびハッシュ値Hk1を、図42に示すメディア・ドライブSAM260を介してROM型の記録媒体1301のセキュアRAM領域132に書き込む。これにより、購入形態が決定されたROM型の記録媒体1301が得られる。このとき、課金処理部187が生成した利用制御データ166および利用履歴データ108は、所定のタイミングで、作業用メモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。なお、ROM型の記録媒体1301のメディアSAM133にキーファイルKF1が格納されている場合には、図42において点線で示されるように、SAM1052はメディアSAM133からキーファイルKF1を

力する。また、この場合に、SAM1052は、作成したキーファイルKF1をメディアSAM133に書き込む。

【0189】<ROM型の記録媒体のコンテンツデータの購入形態を決定した後に、RAM型の記録媒体に書き込む場合の処理>以下、図45に示すように、AV機器1603において購入形態が未決定のROM型の記録媒体1301からセキュアコンテナ104を読み出して新たなセキュアコンテナ104yを生成し、これをAV機器1602に転送し、AV機器1602において購入形態を決定してRAM型の記録媒体1305に書き込む際の処理の流れを図46、図47、図48を参照しながら説明する。なお、ROM型の記録媒体1301からRAM型の記録媒体1305へのセキュアコンテナ104yの転送は、図1に示すネットワーク機器1601およびAV機器1601～1604のいずれの間で行ってもよい。図48は、当該処理のフローチャートである。

【0190】ステップS48-1：SAM1053は、SAM登録リストを検証し、セキュアコンテナの転送先のSAM1052が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS48-2以降の処理を行う。また、SAM1053は、SAM1052がホームネットワーク内のSAMであるか否かの検証も行う。

ステップS48-2：SAM1053とSAM1052との間で相互認証が行われ、セッション鍵データKsesが共有される。

【0191】ステップS48-3：AV機器1603のSAM1053とROM型の記録媒体1301のメディアSAM133との間で相互認証を行い、ROM型の記録媒体1301のメディア鍵データKMD1をSAM1053に転送する。なお、メディア鍵データKMD1を用いた暗号化をROM型の記録媒体1301のメディアSAM133において行う場合には、メディア鍵データKMD1の転送は行わない。

【0192】ステップS48-4：AV機器1602のSAM1052とRAM型の記録媒体1305のメディアSAM133との間で相互認証を行い、RAM型の記録媒体1305のメディア鍵データKMD2をSAM1052に転送する。なお、メディア鍵データKMD2を用いた暗号化をRAM型の記録媒体1305のメディアSAM133において行う場合には、メディア鍵データKMD2の転送は行わない。

【0193】ステップS48-5：SAM1053は、図46に示すように、メディア・ドライブSAM管理部855を介して、ROM型の記録媒体1301のROM領域131からコンテンツファイルCFおよびその署名データSIG6.cpを読み出し、これをSAM管理部190に出力すると共に、署名処理部189において、秘密鍵データKsam3,sを用いて、これらの署名データSIG

350. SAM3を作成する。

【0194】ステップS48-6: SAM1053は、図46に示すように、メディア・ドライブSAM管理部855を介して、ROM型の記録媒体1301のセキュアRAM領域132からキーファイルKFおよびその署名データSIG7.OPを読み出し、これをSAM管理部190に出力すると共に、署名処理部189において、秘密鍵データK_{SAM3}を用いて、これらの署名データSIG352. SAM3が作成される。

【0195】ステップS48-7: SAM1053において、記憶部192からSAM管理部190に公開鍵証明書データCER_{SAM3}およびその署名データSIG351. ESCを読み出される。

【0196】ステップS48-8: SAM1053の例えばSAM管理部190において、図47に示すセキュアコンテナ104yが作成される。

【0197】ステップS48-9: SAM1053の暗号化・復号部171において、ステップS48-2で得たセッション鍵データK_{SES}を用いて、セキュアコンテナ104yが暗号化され、SAM管理部190を介して、AV機器1602のSAM1052に出力される。

【0198】ステップS48-10: SAM1052では、図50に示すように、SAM管理部190を介してSAM1053から入力した図47に示すセキュアコンテナ104yが暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号される。そして、当該復号されたセキュアコンテナ104y内のキーファイルKFおよびその署名データSIG7.OP、SIG

350. SAM3と、公開鍵証明書データCER_{SAM3}およびその署名データSIG351. ESCと、公開鍵証明書データCER_{OP}およびその署名データSIG1. ESCとが、作業用メモリ200に書き込まれる。

【0199】ステップS48-12: SAM1052の署名処理部189において、セキュアコンテナ104y内に格納された署名データSIG6.OP、SIG350. SAM3の正当性、すなわちコンテンツファイルCFの作成者および送信者の正当性を確認する。

ステップS48-13: コンテンツファイルCFの作成者および送信者が正当であると確認された後に、メディア・ドライブSAM管理部855を介してRAM型の記録媒体1305のRAM領域134にコンテンツファイルCFが書き込まれる。

【0200】ステップS48-14: 署名処理部189において、署名データSIG351. ESCが署名検証され、公開鍵証明書データCER_{SAM3}の正当性が確認された後に、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}および公開鍵データK_{ESC.P}を用いて、署名データSIG7.OP、SIG352. SAM3、SIGK1. ESCの正当性、すなわちキーファイルKFの作成者および送信者の正当性が確認される。

【0201】ステップS48-15: キーファイルKFの作成者および送信者の正当性が確認されると、作業用メモリ200からキーファイルKFが読み出されて暗号化・復号部172に出力され、暗号化・復号部172において、ライセンス鍵データKD1~KD3を用いて復号された後に、作業用メモリ200に書き戻される。

【0202】ステップS48-16: 作業用メモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。そして、利用監視部186において、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理(監視)される。

【0203】ステップS48-17: ユーザによる図38に示す購入・利用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。

ステップS48-18: 課金処理部187において、決定された購入・利用形態に応じて利用制御データ166および利用履歴データ108が生成され、これが作業用メモリ200および外部メモリ201にそれぞれ書き込まれる。利用制御データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

【0204】ステップS48-19: コンテンツ鍵データK_Cおよび利用制御データ166が、作業用メモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED2}および購入者鍵データK_{PIN}を用いて順に暗号化され、メディアSAM管理部197に出力される。また、作業用メモリ200からメディアSAM管理部197に、キーファイルKFが出力される。

【0205】ステップS48-20: メディアSAM管理部197において、図34(C)に示すキーファイルKF1が作成され、キーファイルKF1がメディアSAM管理部197を介してRAM型の記録媒体1305のメディアSAM133に書き込まれる。また、メディアSAM管理部197を介して、キーファイルKFがRAM型の記録媒体1305のメディアSAM133に書き込まれる。

【0206】以下、SAM1051~1054の実現方法について説明する。SAM1051~1054の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図22に示す各機能を実現するためのセキュリティ機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密性の高いデータが格納される。暗号ライブラリーモジュール(公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数)、コンテ

ソツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0207】例えば、図22に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。また、図22に示す記憶部192や、図22に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM1051～1054に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。また、SAM1051～1054には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0208】上述したように、SAM1051～1054は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM1051～1054を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Magagement Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。また、SAM1051～1054は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。SAM1051～1054自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0209】SAM1051～1054の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合

と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときのみ解説することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッグ）で実行状況を解説されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（MiniOS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0210】次に、図22に示すAV圧縮・伸長用SAM163について説明する。図22に示すように、AV圧縮・伸長用SAM163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。相互認証部220は、AV圧縮・伸長用SAM163がSAM1051からデータを入力する際に、図23に示す相互認証部170との間で相互認証を行ってセッション鍵データKsesを生成する。

【0211】復号部221は、SAM1051から入力したコンテンツ鍵データKc、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データKsesを用いて復号する。そして、復号部221は、復号したコンテンツ鍵データKcおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0212】復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データKcを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0213】伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。伸長部223は、例えば、図3(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0214】電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータ

Cを再生モジュール169に出力する。このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、AV圧縮・伸長用SAM163において埋め込まれる。なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0215】半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試験時の再生機能を限定したり、試験可能な期間を限定するなどの制御を行う。

【0216】再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0217】次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。図51(A)は、コンテンツプロバイダ101からSAM1051にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod50が送信される。モジュールMod50には、モジュールMod51およびその秘密鍵データKcp,sによる署名データSIGcpが格納されている。モジュールMod51には、コンテンツプロバイダ101の秘密鍵データKcp,pを格納した公開鍵証明書データCERcpと、公開鍵証明書データCERcpに対しての秘密鍵データKesc,sによる署名データSIGescと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERcpを格納したモジュールMod50を、コンテンツプロバイダ101からSAM1051に送信することで、SAM1051において署名データSIGcpの検証を行なう際に、EMDサービスセンタ102からSAM1051に公開鍵証明書データCERcpを送信する必要がなくなる。

【0218】図51(B)、(C)は、コンテンツプロバイダ101からSAM1051にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図51(B)に示すモジュールMod52が送信される。モジュールMod52には、送信するデータDataと、その秘密鍵データKcp,sによる署名データSIGcpとが

格納されている。また、EMDサービスセンタ102からSAM1051には、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図51(C)に示すモジュールMod53が送信される。モジュールMod53には、コンテンツプロバイダ101の公開鍵証明書データCERcpと、その秘密鍵データKesc,sによる署名データSIGescとが格納されている。

【0219】図51(D)は、SAM1051からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod54が送信される。モジュールMod54には、モジュールMod55およびその秘密鍵データKsami,sによる署名データSIGsamiが格納されている。モジュールMod55には、SAM1051の秘密鍵データKsami,pを格納した公開鍵証明書データCERsamiと、公開鍵証明書データCERsamiに対しての秘密鍵データKesc,sによる署名データSIGescと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERsamiを格納したモジュールMod55を、SAM1051からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIGsamiの検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCERsamiを送信する必要がなくなる。

【0220】図51(E)、(F)は、SAM1051からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図51(E)に示すモジュールMod56が送信される。モジュールMod56には、送信するデータDataと、その秘密鍵データKsami,sによる署名データSIGsamiとが格納されている。また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データKsesで暗号化した図51(F)に示すモジュールMod57が送信される。モジュールMod57には、SAM1051の公開鍵証明書データCERsamiと、その秘密鍵データKesc,sによる署名データSIGescとが格納されている。

【0221】図52(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータData

をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod58が送信される。モジュールMod58には、モジュールMod59およびその秘密鍵データKcp,sによる署名データSIGcpが格納されている。モジュールMod59には、コンテンツ

プロバイダ101の秘密鍵データKcp,pを格納した公開鍵証明書データCERcpと、公開鍵証明書データCERcpに対しての秘密鍵データKesc,sによる署名データSIGescと、送信するデータDataとが格納されている。

【0222】図52(H)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データKsesで暗号化した図52(H)に示すモジュールMod60が送信される。モジュールMod60には、送信するデータDataと、その秘密鍵データKcp,sによる署名データSIGcpとが格納されている。このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データCERcpは既に登録されている。

【0223】図52(I)は、SAM1051からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod61が送信される。モジュールMod61には、モジュールMod62およびその秘密鍵データKsami,sによる署名データSIGsamiが格納されている。モジュールMod62には、SAM1051の秘密鍵データKsami,pを格納した公開鍵証明書データCERsamiと、公開鍵証明書データCERsamiに対しての秘密鍵データKesc,sによる署名データSIGescと、送信するデータDataとが格納されている。

【0224】図52(J)は、SAM1051からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図52

(J)に示すモジュールMod63が送信される。モジュールMod63には、送信するデータDataと、その秘密鍵データKsami,sによる署名データSIGsamiとが格納されている。このとき、EMDサービスセンタ102にはSAM1051の公開鍵証明書データCERsamiは既に登録されている。

【0225】以下、SAM1051～1054の出荷時におけるEMDサービスセンタ102への登録処理について説明する。なお、SAM1051～1054の登録処理は同じであるため、以下、SAM1051の登録処理について述べる。SAM1051の出荷時には、EMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図23などに示す記憶部192に以下に示す鍵データが初期登録される。また、SAM1051には、例えば、出荷時に、記憶部192などに、SAM1051がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部192には、例えば、図27において左側に「*」が付されているSAM1051の識別子SAM_ID、記録用鍵データKstr、ルート認証局2の公開鍵データKrc-a、EMDサービスセンタ102の公開鍵データKesc,p、SAM1051の秘密鍵データKsami,s、公開鍵証明書データCERsamiおよびその署名データSIG22,esc、AV圧縮・伸長用SAM163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データCERsamiは、SAM1051を出荷後に登録する際にEMDサービスセンタ102からSAM1051に送信してもよい。

【0226】また、記憶部192には、SAM1051の出荷時に、図3に示すコンテンツファイルCFおよびキーファイルKFを読み込み形式を示すファイルリダが、EMDサービスセンタ102によって書き込まれる。SAM1051では、コンテンツファイルCFおよびキーファイルKFに格納されたデータを利用する際に、記憶部192に記憶されたファイルリダが用いられる。

【0227】ここで、ルート認証局2の公開鍵データKrc-aは、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データKrc-aは、図1に示すルート認証局2によって発行される。また、EMDサービスセンタ102の公開鍵データKesc,pは、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データKesc,pは192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データKesc,pを登録する。また、ルート認証局92は、公開鍵データKesc,pの公開鍵証明

書データCEREScを作成する。公開鍵データKESc.Pを格納した公開鍵証明書データCEREScは、好ましく、SAM1051の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データCEREScは、ルート認証局92の秘密鍵データKROOT.sで署名されている。

【0228】EMDサービスセンタ102は、乱数を発生してSAM1051の秘密鍵データKsAM1.s、を生成し、これとペアとなる公開鍵データKsAM1.pを生成する。また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データKsAM1.pの公開鍵証明書データCERsAM1を発行し、これに自らの秘密鍵データKESc.sを用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

【0229】また、SAM1051には、EMDサービスセンタ102により、EMDサービスセンタ102の管理下にある一意（ユニーク）な識別子SAM_IDが割り当てられ、これがSAM1051の記憶部192に格納されると共に、EMDサービスセンタ102によって管理される。

【0230】また、SAM1051は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192にライセンス鍵データKD1~KD3が転送される。すなわち、SAM1051を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM1051を搭載している機器（当該例では、ネットワーク機器1601）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報（ユーザの氏名、住所、連絡先、性別、決済口座、ログイン名、パスワードなど）を記載して例えば郵便などのオフラインで行なわれる。SAM1051は、上述した登録手続を経た後でないと使用できない。

【0231】EMDサービスセンタ102は、SAM1051のユーザによる登録手続に応じて、ユーザに固有の識別子USER_IDを発行し、例えば、SAM_IDとUSER_IDとの対応関係を管理し、課金時に利用する。また、EMDサービスセンタ102は、SAM1051のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行ったり、オフラインで本人の確認を行なう。

【0232】次に、図27に示すように、SAM1051内の記憶部192にSAM登録リストを格納する手順について説明する。図1に示すSAM1051は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM1052~SAM1054のSAM登録リストを得る。なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図53に示すように、バス191にSAM1051~1054に加えてAV機器1605、1606のSCMS処理回路1055、1056が接続されている場合に、SAM1051~1054およびSCMS処理回路1055、1056を対象として生成される。従って、SAM1051は、当該トポロジーマップから、SAM1051~1054についての情報を抽出して図54に示すSAM登録リストを生成する。

【0233】そして、SAM1051は、図54に示すSAM登録リストを、EMDサービスセンタ102に登録して署名を得る。これらの処理は、バス191のセッションを利用してSAM1051が自動的に行き、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。EMDサービスセンタ102は、SAM1051から図54に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM1051より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、予め保持している図55に示すリボケーションリストCRLをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。各SAMは他のSAMと通信を行う際に、リボケーションリストによって通信相手のSAMが無効にされている場合には、当該通信相手のSAMとの通信を停止する。また、EMDサービスセンタ102は、決済時にはSAM1051に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。これにより、図56に示すSAM登録リストが作成される。なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0234】なお、リボケーションリストCRLの更新は、例えば、EMDサービスセンタ102からSAMに放送される更新データに応じて、SAM内部で自動的に

行なうことが好ましい。

【0235】以下、SAMが持つセキュリティ機能について説明する。SAMは、セキュリティに関する機能として、共通鍵暗号方式のDES (Triple DES/AES)、公開鍵暗号方式の楕円曲線暗号(署名生成/検証ECDSA, 共有鍵生成EC-DH, 公開鍵暗号EC-Elgamal), 圧縮関数のハッシュ関数SHA-1, 乱数生成器(真性乱数)の暗号ライブラリーのIP部品を有している。相互認証、署名生成、署名検証、共有鍵(セッション鍵)作成(配送)には公開鍵暗号方式(楕円曲線暗号)が用いられ、コンテンツの暗号、復号には共通鍵暗号(DES)が用いられ、署名生成、検証の中のメッセージ認証に圧縮関数(ハッシュ関数)が用いられる。

【0236】図57は、SAMが持つセキュリティ機能を説明するための図である。SAMが管理するセキュリティ機能は、コンテンツに関連する暗号、復号処理をつかさどるアプリケーション層でのセキュリティ機能(1)と、通信相手と相互認証をしてセキュアな通信路を確保する物理層のセキュリティ機能(2)との2種類がある。EMDシステム100では、配信されるコンテンツデータCはすべて暗号化され、決済と同時に鍵の購入手続きをすることを前提としている。権利書データ106は、コンテンツデータCと一緒にイン・バンド方式で送られることを前提としているので、ネットワークの媒体と関係のない層でそのデータが管理され、衛星、地上波、ケーブル、無線、記録媒体(メディア)などの流通経路によらず、共通な権利処理システムを提供できる。具体的には、権利書データ106をネットワークの物理層のプロトコルのヘッダに挿入したりすると、使用するネットワークによって、挿入するデータが同じで、ヘッダのどこに挿入するかを各々のネットワークで決めないといけない。

【0237】本実施形態では、コンテンツデータCおよびキーファイルKFの暗号化は、アプリケーション層での保護を意味している。相互認証は、物理層やトランスポート層で行ってもよいし、アプリケーション層で行ってもよい。物理層に暗号機能を組み込むことは、使用するハードウェアに暗号機能を組み込むことを意味している。送信、受信の両者間のセキュアの通信路を確保することが相互認証の本来の目的なので物理層で実現できることが望ましいが、実際はトランスポート層で実現し、伝送路によらないレベルでの相互認証が多い。

【0238】SAMが実現するセキュリティ機能には、通信先の相手の正当性を確認するための相互認証と、アプリケーション層での課金処理をともなうコンテンツデータの暗号化および復号とがある。機器間で通信を行う際のSAM相互間での相互認証は、通常、アプリケーション層レベルに実装されるが、トランスポート層や物理層などの他のレイヤに実装されてもよい。物理層に実装する相互認証は、5C1394CP(Content Protecti

on)を利用する。1394CPは1394LINKIC(ハードウェア)のIsochronous Channelに共通鍵暗号であるM6が実装されており、Asynchronous Channelによる相互認証(楕円曲線暗号、ハッシュ関数を利用した共通鍵暗号)の結果、生成されるセッション鍵をIsochronous ChannelのM6に転送し、M6による共通鍵暗号を実現する。

【0239】SAM相互間の相互認証を物理層のハードウェア上に実装する場合には、公開鍵暗号(楕円曲線暗号)を利用した相互認証で生成されたセッション鍵をホストCPUを介して1394LINKICのM6に転送し、1394CPで生成されたセッション鍵と併用してコンテンツデータの暗号化を行う。また、SAM相互間の相互認証をアプリケーション層で行う場合には、SAM内部の共通鍵暗号ライブラリ(DES/Triple DES/AES)を使って暗号化を行う。

【0240】本実施形態では、例えば、SAM相互間の相互認証をアプリケーション層に実装し、1394CPによる相互認証を1394LINKICという物理層(ハードウェア)に実装する。この場合に、課金処理をともなうコンテンツデータの暗号化および復号はアプリケーション層でおこなわれるが、アプリケーション層は一般ユーザから簡単にアクセスでき、時間無制限に解析される可能性があるため、当該課金処理をともなう処理に関しては、本実施形態では、外部から処理内容をいっさいモニタ(監視)できない耐タンパ性を持ったハードウェア内部で行っている。これがSAMを耐タンパ性の構造を持ったハードウェアで実現する最大の理由である。なお、当該課金処理をホストCPU内で行う場合は、CPUに耐タンパ性のソフトウェアを実装する。

【0241】図58は、コンテンツプロバイダ101からネットワーク機器1601に送信されたセキュアコンテンツ104に格納されたコンテンツデータCをAV機器(ストレージ機器)1601において記録媒体(メディア)に書き込む際に行われる、コンテンツプロバイダ101およびSAM1051におけるセキュリティ機能を説明するための図である。コンテンツプロバイダ101からネットワーク機器1601に送信されるセキュアコンテンツ104内のコンテンツデータCは、コンテンツプロバイダ101が管理しているコンテンツ鍵データKcで暗号化されている。コンテンツ鍵データKcおよび権利書データ106は、EMDサービスセンタ102が管理するライセンス鍵データKDで暗号化されている。図58に示す例では、セキュアコンテンツ104が、ネットワークの物理層のプロトコルでカプセル化され、クライアントのネットワーク機器1601にダウンロードされる。その過程で、コンテンツプロバイダ101およびSAM1051において乱数を生成し、公開鍵暗号方式と共通鍵暗号方式とを併用して相互認証をおこなう。そして、ネットワーク機器1601において、ダウンロード

されたセキュアコンテナ 104 が、メディアに記録される。このとき、購入形態が決定され、コンテンツ鍵データ Kc および権利書データ 106 がライセンス鍵データ KD を用いて暗号化された後にメディアに記録され、利用制御データ 166 がメディア鍵データ Kmed および記録用鍵データ Kstr を用いて暗号化された後にメディアに記録される。

【0242】図 59 (A) は一般的に用いられる OSI 参照モデルにおける送信側および受信側の各層 (レイヤー) で行われる通信を説明するための図、図 59 (B) は図 58 に示すコンテンツプロバイダ 101 とネットワーク機器 160₁ (SAM105₁) との間での通信時の保護機能を詳細に説明するための図である。図 59

(A) に示すように、OSI 参照モデルでは、送信側および受信側において物理層、データリンク層、トランスポート層、・・・、ソケット層およびアプリケーション層が下から上に順に構築され、対応するレイヤ相互間でデータのやりとりが行われる。また、コンテンツプロバイダ 101 とネットワーク機器 160₁ (SAM105₁) との間の通信は、図 59 (B) に示す階層構造に基づいて行われる。図 59 (B) に示す例では、物理層として HDLC, V. 23 および/または X. 25 などが用いられ、トランスポート層として IP などが用いられ、ソケット層として Socket (API) などが用いられ、アプリケーション層として http, XML/SMIL/HTML などが用いられ、各層が独自のセキュリティ機能を有している。

【0243】ここで、物理層では伝送路上の保護が行われ、当該伝送路を伝送するアプリケーションに関するデータを保護できる。当該物理層での保護は、ハードウェアでの保護機能の実装が前提になる。トランスポート層での保護は、伝送路には依存しないが、トランスポートプロトコルを使用している全てのアプリケーションに関するデータについて行われる。ソケット層での保護は、当該ソケットを利用しているアプリケーションに関する全てのデータについて行われる。アプリケーション層での保護は、全てのアプリケーションに関するデータを保護することができるが、一般ユーザによる解析、改竄の可能性が高い。

【0244】ネットワーク経由の処理には、すくなくとも 2 つのプログラムが存在する。一つはローカルにあるプラットフォーム上で動くプログラムで、ユーザが操作する。もう一つはサービスを提供するプログラム (アプリケーション) で、ネットワークを介した通信先にある (リモート) プラットフォーム上で動くものである。図 59 (A), (B) に示すように、各レイヤーがお互いの上下の要素とやりとりすることにより、結果的に通信が可能になる。下側の要素との間で受け渡される情報は、対応するレベルの要素と直接やりとりしている、とみることができる。つまり、送信側の物理層は、受信側

の物理層と、送信側のアプリケーションは、受信側のアプリケーションと通信しているようにみえる。

【0245】送信、受信の間で情報を保護するには、図 59 (A), (B) に示すように、直接やりとりするレイヤー間で保護する仕組みを作ればよい。これは送信側のあるレイヤーで情報を暗号化することは、受信側の対応するレイヤーでないと復号できないことを意味する。その場合、アプリケーション層、トランスポート層、データリンク層、・・・、物理層の各レイヤーで暗号化して保護する。物理層での保護は、ハードウェアレベルでの保護になる。ネットワークでは伝送路のハードウェアに依存するところを暗号化する。パッケージでは記録媒体 (メディア) に関連するハードウェア部に絡んだ部分を暗号化する。データリンク層 (MAC 層) は、比較的物理層に依存しているレイヤーなので物理層での保護の範疇に入れる。トランスポート層は、TCP/IP の IP パケットレベルでの保護になる。これは IP パケットでの保護機能である IP Sec が有名である。この方式の場合は、相手も同じ機構 (IP Sec) を用意していれば、パケットに含まれるすべての情報が保護できる。ただし、パケットレベルでの処理にはカーネルの再構築が必要である。ソケットレベルでの保護には、例えば、SSL (Secure Socket Layer) が用いられる。Socket API は TCP/IP 関連のアプリケーションソフトを書くとき、このソケットを利用して書くための一種の API 層で、このレベルでの保護は、そのソケットを利用するすべてのアプリケーションを保護できることを意味している。逆にそのソケットを利用しないアプリケーションは保護できない。最後にアプリケーションレベルでの保護は、アプリケーションの内部でデータを保護する方式である。これを利用すれば伝送路に依存せず、すべてのアプリケーションを保護することができる。

【0246】アプリケーションレベルで保護するプログラムは、カーネルを再構築する必要がなく、簡単にシステムを構築できるため、頻繁に使用される。そうすると、すべてアプリケーション層でデータを暗号化すれば、簡単で問題ないように思われるがアプリケーション層は一般ユーザが唯一操作できるレイヤーで、時間無制限にハッカー (暗号解読) できるチャンスがある。逆にカーネル、あるいはハードウェアに依存した暗号化は、一般ユーザから操作できない部分であり、この部分に依存した暗号化は非常に強固である。カーネル、ハードウェアに依存したレイヤーでの暗号化は、送信、受信間で、両方ともその暗号化に対応するシステムでないと成立しない。

【0247】図 60 は、図 58 に示すネットワーク機器 160₁ (SAM105₁) と AV 機器 160₂ (SAM105₂) との間での通信時の保護機能を詳細に説明するための図である。図 60 に示すように、AV 機器 160₂ (SAM105₂) では、物理層としてセクタおよ

びファイルシステムが用いられ、トランスポート層としてIPが用いられ、トランスポート層とアプリケーション層の間にHAViなどのホームネットワークミドルウェアが用いられている。ここで、物理層（セクタ）からアプリケーション層までの全ての層の通信データは記録媒体（メディア）に記録される際にメディア鍵データK_{MED}を用いて暗号化されていることで保護され、ファイルシステムからアプリケーション層までの全ての層の通信データは記録媒体に記録される際に記録用鍵データK_{STR}を用いて暗号化されて保護される。

【0248】ネットワーク機器160₁が受信したコンテンツデータを、AV機器160₂において記録媒体（メディア）に記録する場合、ハードウェアと記録媒体という物理層でのセキュリティ保護が必要になる。このような物理層でのセキュリティ保護を実現するために、本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}の2種類を鍵データを定義する。記録用鍵データK_{STR}は、機器の種類ごとに定義されている鍵でセクタレベルの物理層を除いたアプリケーション層からトランスポート層まで、どのレイヤーで暗号化してもよい。記録用鍵データK_{STR}はSAM内に格納されており、SAM内で記録用鍵データK_{STR}を用いた暗号化および復号が行なわれる。

【0249】メディア鍵データK_{MED}は、各記録媒体に定義されている鍵で、個々の記録媒体毎に定義および記録されている。メディア鍵データK_{MED}を用いた暗号化は、どのレイヤーで行なってもよいが、記録媒体という物理層レベルでの保護が前提の鍵なので、記録媒体の物理層に依存した部分に実装するのがより良い。例えば、記録媒体上に暗号化および復号を行なうメディアSAMがあり、当該メディアSAMにおいて暗号化および復号することが望ましい。あるいは、機器側の記録媒体の物理層に関連する信号処理部分にハードウェアとして実装し、そこにメディア鍵データを記録媒体から転送して（相互認証が必要）、暗号化および復号を行なってもよい。記録媒体の物理層に依存しない部分で暗号化および復号を行なうには、SAMと相互認証をして、生成されたセッション鍵データK_{SES}でメディア鍵データK_{MED}を暗号化して機器側のSAMに転送し、そこで暗号化および復号を行なってもよい。これは、鍵の定義のみで、メディア上という物理層レベルを保護していることになる。

【0250】図61は、例えば、図1に示すAV機器160₂において図11に示すROM型の記録媒体130₁からコンテンツデータCを再生し、当該再生したコンテンツデータをバス191を介してAV機器160₃に伝送し、AV機器160₃において図14に示すRAM型の記録媒体130₄に記録する場合のセキュリティ処理を説明するための図である。以下に示す(A)～

(M)は、当該処理の手順を示し、図61に示された符

号と対応している。

【0251】(A)：再生側のAV機器160₂とROM型の記録媒体130₁のメディアSAM133₁との間で相互認証を行う。

(B)：記録側のAV機器160₃とRAM型の記録媒体130₄のメディアSAM133₄との間で相互認証を行う。のメディア(Media-SAM)とSAMとで相互認証。

(C), (D)：AV機器160₂とAV機器160₃

との間で1394シリアルバスの機能を用いた相互認証（機器間認証）を行い、両者でセッション鍵データK_{SES}を共有する。

(E), (F)：上記(A), (B)の認証結果を使用して、SAM105₂とSAM105₃との間の相互認証(End to End 認証)を行い、セッション鍵が共有される

【0252】(G)：メディアSAM133₁あるいはSAM105₂によって、ROM領域131から読み出されたコンテンツファイルCFおよびキーファイルKFが、メディア鍵データK_{MED2}を用いて復号（開錠）される。

(H)：SAM105₂によって、コンテンツファイルCFおよびキーファイルKFが、記録用鍵データK_{STR2}を用いて復号される。

(I)：SAM105₂において、コンテンツファイルCFに格納されたコンテンツデータの再生、記録に伴う署名検証および購入形態決定処理などの権利処理が行われる。なお、コンテンツデータCの再生時には、コンテンツ鍵データK_Cによる復号処理が行われる。

(J)：コンテンツファイルCFおよびキーファイルKFが、AV機器160₂において上記(E), (F)および(C), (D)で生成されたセッション鍵データK_{SES}を用いて暗号化され、AV機器160₃に送信され、AV機器160₃において同じセッション鍵データK_{SES}を用いて復号される。

【0253】(K)：SAM105₂で権利処理が行なわれていない場合には、SAM105₃で権利処理が行なわれる。

(L)：SAM105₃において、コンテンツファイルCFおよびキーファイルKFが、記録用鍵データK_{STR2}を用いて暗号化される。

(M)：SAM105₃あるいはメディアSAM133₄において、コンテンツファイルCFおよびキーファイルKFが、メディア鍵データK_{MED}を用いて暗号化され、RAM型の記録媒体130₄のRAM領域134に記録される。

【0254】以下、図1に示すユーザホームネットワーク103内の例えばネットワーク機器160₁内での各種のSAMに搭載形態の一例を図62を参照しながら説明する。図62に示すように、ネットワーク機器160

1 内には、ホストCPU810₁、SAM105₁、ダウンロードメモリ167、メディア・ドラブSAM260、ドライブCPU1003、DRAMなどのショックプルーフ(Shock Proof)メモリ1004を有する。ダウンロードメモリ167と、ショックプルーフメモリ1004の一部の記憶領域は、SAM105₁およびホストCPU810₁の双方からアクセス可能な共有メモリとして用いられる。ダウンロードメモリ167は、メモリコントローラ、バスアービターおよびブリッジの機能を持つモジュール1005を介して、ホストCPUバス1000に接続されている。ダウンロードメモリ167およびショックプルーフメモリ1004には、前述したコンテンツファイルCFおよびキーファイルKFなどが記憶される。ショックプルーフメモリ1004の記憶領域のうち共有メモリとしては用いられる記憶領域以外の記憶領域は、データバス1002を介してメディア・ドラブSAM260から入力したコンテンツデータをAV圧縮・伸長用SAM163に出力するまで一時的に記憶するために用いられる。

【0255】AV圧縮・伸長用SAM163は、ホストCPUバス1000を介してダウンロードメモリ167との間でデータ転送を行い、データバス1002を介してメディア・ドラブSAM260との間でデータ転送を行う。

【0256】ホストCPUバス1000には、ダウンロードメモリ167の他に、SAM105₁、AV圧縮・伸長用SAM163およびDMA(Direct Memory Access)1010が接続されている。DMA1010は、ホストCPUバス1000を介したダウンロードメモリ167へのアクセスを、ホストCPU810₁からの命令に応じて、統括的に制御する。また、ホストCPUバス1000は、1394シリアル・インターフェースのLINK層を用いてユーザホームネットワーク103内の他のSAM105₂~105₄と通信を行なう際に用いられる。

【0257】ドライブCPUバス1001には、ドライブCPU1003、メディア・ドラブSAM260、RFアンプ1006、メディアSAMインターフェイス1007およびDMA1011が接続されている。ドライブCPU1003は、例えば、ホストCPU810₁からの命令を受けて、ディスク型の記録媒体130にアクセスを行う際の処理を統括的に制御する。この場合に、ホストCPU810₁がマスタとなり、ドライブCPU1003がスレーブとなる。ドライブCPU1003は、ホストCPU810₁から見てI/Oとして扱われる。ドライブCPU1003は、例えばRAM型などの記録媒体130にアクセスを行う際のデータのエンコードおよびデコードを行う。ドライブCPU1003は、RAM型の記録媒体130がドライブにセットされると、RAM型の記録媒体130がSAM105₁による

権利処理の対象となる(EMDシステム100の対象となる)記録媒体であるか否かを判断し、当該記録媒体であると判断した場合に、そのことをホストCPU810₁に通知すると共に、メディア・ドラブSAM260にメディアSAM133との間の相互認証などを行うことを指示する。

【0258】メディアSAMインターフェイス1007は、ドライブCPUバス1001を介した記録媒体130のメディアSAM133に対してのアクセスを行う際のインターフェイスとして機能する。DMA1011は、例えば、ドライブCPU1003からの命令に応じて、ドライブCPUバス1001およびデータバス1002を介したショックプルーフメモリ1004へのメモリアccessを統括的に制御する。DMA1011は、例えば、データバス1002を介した、メディア・ドラブSAM260とショックプルーフメモリ1004との間のデータ転送を制御する。

【0259】図62に示す構成では、例えば、SAM105₁と記録媒体130のメディアSAM133との間で相互認証などの通信を場合には、ホストCPU810₁の制御に基づいて、ホストCPUバス1000、ホストCPU810₁、ドライブCPU1003内のレジスタ、ドライブCPUバス1001およびメディアSAMインターフェイス1007を介して、SAM105₁とメディアSAM133との間でデータが転送される。また、記録媒体130にアクセスを行う場合には、メディア・ドラブSAM260とメディアSAM133との間で相互認証が行われる。また、前述したように、ダウンロードメモリ167およびショックプルーフメモリ1004にアクセスを行うために、AV圧縮・伸長用SAM163においてデータを圧縮または伸長する場合には、SAM105₁とAV圧縮・伸長用SAM163との間で相互認証が行われる。

【0260】本実施形態では、図62において、SAM105₁およびAV圧縮・伸長用SAM163は、ホストCPU810₁からは、I/Oインターフェイスに接続されたデバイスとして扱われる。SAM105₁およびAV圧縮・伸長用SAM163とホストCPU810₁との間の通信およびデータ転送は、メモリI/O&アドレスデコード1020の制御に基づいて行われる。このとき、ホストCPU810₁がマスタ(Master)になり、SAM105₁およびAV圧縮・伸長用SAM163がスレーブ(Slave)になる。SAM105₁およびAV圧縮・伸長用SAM163は、ホストCPU810₁からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をホストCPU810₁に通知する。また、メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からはI/Oインターフェイスに接続されたデバイスとして扱われる。メディアSAM133およびメディア・ドラブSA

M260とドライブCPU1003との間の通信およびデータ転送は、メモリI/O&アドレスデコーダ1021の制御に基づいて行われる。このとき、ドライブCPU1003がマスタになり、メディアSAM133およびメディア・ドラブSAM260がスレーブになる。メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をドライブCPU1003に通知する。

【0261】また、ダウンロードメモリ167およびショックブルーフメモリ1004に対してのコンテンツファイルCFおよびキーファイルKFに関するアクセス制御は、SAM105iが統括的に行ってよいし、あるいはコンテンツファイルCFのアクセス制御をホストCPU810iが行い、キーファイルKFのアクセス制御をSAM105iが行ってもよい。

【0262】ドライブCPU1003によって記録媒体130から読み出されたコンテンツデータCは、RFアンプ1006およびメディア・ドラブSAM260を経て、ショックブルーフメモリ1004に格納され、その後、AV圧縮・伸長用SAM163において伸長される。伸長されたコンテンツデータはD/A変換器において、2でデジタルからアナログに変換され、当該変換によって得られたアナログ信号に応じた音響がスピーカから出力される。このとき、ショックブルーフメモリ1004は、記録媒体130の離散的に位置する記録領域から非連続的に読み出された複数のトラックのコンテンツデータCを一時的に格納した後に、AV圧縮・伸長用SAM163に連続して出力してもよい。

【0263】以下、ユーザホームネットワーク103内の各種のSAMが上述した機能を実現するために備える回路モジュールについて説明する。ユーザホームネットワーク103内のSAMとしては、前述したように、購入形態の決定などの権利処理（利益分配）に係わる処理を行うSAM105（105i～105d）と、記録媒体に設けられるメディアSAM133と、AV圧縮・伸長用SAM163と、メディア・ドラブSAM260とがある。以下、これらのSAMに設けられる回路モジュールをそれぞれ説明する。

【0264】＜権利処理用のSAMの第1形態＞図63は、権利処理用のSAM105aの回路モジュールを説明するための図である。図63に示すように、SAM105aは、CPU1100、DMA1101、MMU1102、I/Oモジュール1103、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、（真性）乱数発生器1110、リアルタイムクロックモジュール1111、外部バスI/F1112を有する耐タンパ性のハードウェア（Tamper Resistant H/W）（本発明の

回路モジュール）である。ここで、CPU1100が本発明の演算処理回路に対応し、DMA1101が本発明の記憶回路制御回路に対応し、MMU1102が本発明の記憶管理回路に対応し、I/Oモジュール1103が本発明のインターフェイスに対応し、マスクROM1104、不揮発性メモリ1105および作業用RAM1106が本発明の記憶回路に対応し、公開鍵暗号モジュール1107が本発明の公開鍵暗号回路に対応し、共通鍵暗号モジュール1108が本発明の共通鍵暗号回路に対応し、ハッシュ関数モジュール1109が本発明のハッシュ値生成回路に対応し、（真性）乱数発生器1110が本発明の乱数生成回路に対応し、リアルタイムクロックモジュール1111が本発明のリアルタイムクロックに対応し、外部バスI/F1112が本発明の外部バスインターフェイスに対応している。

【0265】図23に示すSAM105iの機能モジュールと、図63に示す回路モジュールとの関係を簡単に説明する。CPU1100は、例えば、マスクROM1104および不揮発性メモリ1105に記憶されたプログラムを実行して、図23に示す課金処理部187および利用監視部186の機能を実現する。DMA1101は、CPU1100からの命令に応じて、図22に示すダウンロードメモリ167および図23に示す記憶部192に対してのアクセスを統括的に制御する。MMU1102は、図22に示すダウンロードメモリ167および図23に示す記憶部192のアドレス空間を管理する。I/Oモジュール1103は、例えば、図23に示すメディアSAM管理部197の一部の機能を実現する。マスクROM1104には、SAM105aの初期化プログラムやインテグリティチェック（Integrity Check）プログラムなどの改変しないプログラムおよびデータが製造時に記憶され、図23に示す記憶部192の一部の機能を実現する。不揮発性メモリ1105は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶し、図23に示す記憶部192の一部の機能を実現する。作業用RAM1106は、図23に示す作業用メモリ200に対応している。

【0266】公開鍵暗号モジュール1107は、図23に示す署名処理部189の機能の一部を実現し、例えば、公開鍵暗号方式を用いた、メディアSAM133等と間の相互認証、SAM105の署名データの作成、署名データ（EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ）の検証、データ量の少ないデータ（キーファイルKFなど）の転送を行う際の当該データの暗号化および復号、並びに、鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよいし（H/W IP Solution）、不揮発性メモリ1105に記憶した公開鍵暗号プログラムをCPU1100において実行して実現してもよい（S

/W IPSolution)。

【0267】共通鍵暗号モジュール1108は、図23に示す署名処理部189、暗号化・復号部171、172、173の機能の一部を実現し、相互認証、相互認証によって得た共通鍵であるセッション鍵データKsesを用いたデータの暗号化および復号を行う際に用いられる。共通鍵暗号方式は、公開鍵暗号方式に比べて高速処理が可能であり、例えば、コンテンツデータ（コンテンツファイルCF）などのデータ量が大きいデータを暗号化および復号する際に用いられる。共通鍵暗号モジュール1108は、回路モジュールとして実現してもよいし（H/W IP Solution）、不揮発性メモリ1105に記憶した共通鍵暗号プログラムをCPU1100において実行して実現してもよい（S/W IP Solution）。なお、相互認証は、公開鍵暗号モジュール1107による暗号・復号および共通鍵暗号モジュール1108による暗号・復号の何れか一方あるいは双方を採用する。

【0268】ハッシュ関数モジュール1109は、図23に示す署名処理部189の機能の一部を実現し、署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール1109は、コンテンツプロバイダ101およびEMDサービスセンタ102などの署名データや、図37に示すセキュアコンテナ104xのキープファイルKF1のハッシュ値Hx1を検証する際に用いられる。ハッシュ関数モジュール1109は、回路モジュールとして実現してもよいし（H/W IPSolution）、不揮発性メモリ1105に記憶したハッシュ回路モジュールをCPU1100において実行して実現してもよい（S/W IP Solution）。

【0269】乱数発生器1110は、例えば、図23に示す相互認証部170の機能の一部を実現する。リアルタイムクロックモジュール1111は、リアルタイムの時刻を発生する。当該時刻は、例えば、有効期限付きのライセンス鍵データKDを選択する場合や、利用制御データ166によって示される有効期限の要件を満たされているか否かを判断する際に用いられる。外部バスI/F1112は、図23に示すコンテンツプロバイダ管理部180、ダウンロードメモリ管理部182およびEMDサービスセンタ管理部185の一部を機能を実現する。

【0270】図64は、SAM105a内のハードウェア構成を説明するための図である。図64において、図63に示したものと同一回路モジュールには、図63と同じ符号を付している。図64に示すように、SAM105a内では、SAM・CPUバス1120を介してCPU1100、マスクROM1104および不揮発性メモリ1105が接続されている。内部バス1121には、DMA1101が接続されている。内部バス1122には、I²C・インターフェイス1130、メディアSAM・インターフェイス1131、MS (Memory Stic

k)・インターフェイス1132およびICカード・インターフェイス1133が接続されている。メディアSAM・インターフェイス1131は記録媒体130のメディアSAM133との間でデータ転送を行う。MS・インターフェイス1132はメモリスティック1140との間でデータ転送を行う。ICカード・インターフェイス1133はICカード1141との間でデータ転送を行う。

【0271】外部バス1123には、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、乱数発生器1110、リアルタイムクロック生成モジュール1111および外部バスI/F1112が接続されている。

【0272】SAM・CPUバス1120と内部バス1121とは、バス・インターフェイス116を介して接続されている。内部バス1122と内部バス1121とは、バス・インターフェイス1117を介して接続されている。内部バス1121と外部バス1123とは、バス・インターフェイス1115を介して接続されている。

【0273】DMA1101は、CPU1100からの命令に応じて、内部バス1121を介した、マスクROM1104、不揮発性メモリ1105および作業用RAM1106に対してのアクセスを統括的に制御する。MMU1113は、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、図62に示すダウンロードメモリ167のメモリ空間を管理する。アドレスデコーダ1114は、内部バス1121と外部バス1123との間でデータ転送を行う際に、アドレス変換を行う。また、書き込みロック制御回路1135は、CPU1100からのロック鍵データに基づいて、フラッシュROMに対してのデータの書き込みおよび消去をブロック単位で管理する。

【0274】＜権利処理用のSAMの第2形態＞図65は、権利処理用のSAM105bの回路モジュールを説明するための図である。図65では、SAM105aの構成要素と同じものには、図64と同じ符号を付している。図65に示すように、SAM105bは、セキュアメモリ105ba、ホストCPU810、耐タンパ性ソフトウェア1130、I/Oモジュール1103を用いて実現される。SAM105bでは、ホストCPU810において、耐タンパ性ソフトウェア1130を実行することで、図63に示すCPU1100と同じ機能を実現する。耐タンパ性ソフトウェア1130は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解説および書き換え困難なソフトウェアである。セキュアメモリ105baには、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール110

9、(真性)乱数発生器1110、リアルタイムクロックモジュール1111および外部バスI/F1112を有する耐タンパ性のハードウェアである。なお、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108およびハッシュ関数モジュール1109は、回路モジュールとして実現してもよい(H/W IP Solution)、それぞれ不揮発性メモリ1105に記憶した公開鍵暗号プログラム、共通鍵暗号プログラムおよびハッシュ関数プログラムをホストCPU810において実行して実現してもよい(S/W IP Solution)。

【0275】以下、前述したメディアSAM133として機能する各種のメディアSAMの構成について説明する。

<メディアSAMの第1形態>図66は、メディアSAM133aの回路モジュールを説明するための図である。図66に示すように、メディアSAM133aは、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、共通鍵暗号モジュール1208、ハッシュ関数モジュール1209、(真性)乱数発生器1210を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0276】CPU1200は、耐タンパ性のハードウェア内の各回路の制御を行う。

【0277】公開鍵暗号モジュール1207は、例えば、公開鍵暗号方式を用いた、例えば(1):図62に示すSAM1051およびドライブCPU1003等と間の相互認証、(2)メディアSAM133の署名データの作成、署名データ(EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ)の検証、

(3):転送されるデータ量の少ないメッセージの暗号化および復号、並びに、(4):相互認証によって得たセッション鍵データKsesの鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶した公開鍵暗号プログラムをCPU1200において実行して実現してもよい(S/W IP Solution)。

【0278】共通鍵暗号モジュール1208は、相互認証、相互認証によって得た共通鍵であるセッション鍵データKsesを用いたキーファイルKF、KF1などのデータの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1208は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶した共通鍵暗号プログラムをCPU1200において実行して実現してもよい(S/W IP Solution)。なお、相互認証は、公開鍵暗号モジュール1207による暗号・復号および共通鍵暗号モジュール1208によ

る暗号・復号の何れか一方あるいは双方を採用する。

【0279】ハッシュ関数モジュール1209は、データのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール1109は、図37に示すセキュアコンテナ104xのキーファイルKF1のハッシュ値Hk1を検証する際に用いられる。ハッシュ関数モジュール1209は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶したハッシュ回路モジュールをCPU1200において実行して実現してもよい(S/W IP Solution)。

【0280】乱数発生器1210は、例えば、相互認証を行う際に用いられる。I/Oモジュール1203は、図62に示すメディアSAM1/F1007との間の通信を行う際に用いられる。

【0281】マスクROM1204には、メディアSAM133aの初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムおよびデータが製造時に記憶される。不揮発性メモリ1205は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

【0282】図67は、メディアSAM133aがROM型の記録媒体に搭載される場合に、メディアSAM133aの出荷時にマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図67に示すように、ROM型の記録媒体の出荷時には、メディアSAM133aには、メディアSAMの識別子(ID)、記録用鍵データKSTR(メディア鍵データKmed)、EMDサービスセンタ102の公開鍵データKesc.p、ルート認証局92の公開鍵データKR-GA.p、メディアSAM133aの公開鍵証明書データCERMSAM、メディアSAM133aの公開鍵データKMSAM.p、メディアSAM133aの秘密鍵データKMSAM.s、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子(ID)、メディアのタイプ(メディアの種別情報、ROMおよびRAMの何れかを特定する情報)、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、所定の検証値(MAC値)などが記憶される。ここで、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、並びに所定の検証値(MAC値)は、EMDサービスセンタ102が管理するライセンス鍵データKDを用いて暗号化されている。

【0283】図68は、メディアSAM133aがROM型の記録媒体に搭載される場合に、メディアSAM133aの出荷後のユーザ登録およびコンテンツデータの購入形態決定を行ったときにマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図68に示すように、メディアSAM13

3 a には、ユーザ登録によって、新たに、ユーザID、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報、キーファイルKF₁などのデータが書き込まれる。

【0284】図69は、メディアSAM133aがRAM型の記録媒体に搭載される場合に、メディアSAM133aの出荷時にマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図69に示すように、RAM型の記録媒体の出荷時には、メディアSAM133aには、メディアSAMの識別子（ID）、記録用鍵データKSTR（メディア鍵データKMED）、EMDサービスセンタ102の公開鍵データKESC.P、ルート認証局92の公開鍵データR-GA.P、メディアSAM133aの公開鍵証明書データCERMSAM、メディアSAM133aの公開鍵データKMSAM.P、メディアSAM133aの秘密鍵データKMSAM.S、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子（ID）、メディアのタイプ（メディアの種別情報、ROMおよびRAMの何れかを特定する情報）が記憶されており、キーファイルKFの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータC（コンテンツファイルCF）のキーファイルKF、KF₁、所定の検証値（MAC値）などは記憶されていない。

【0285】図70は、メディアSAM133aがRAM型の記録媒体に搭載される場合に、メディアSAM133aの出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図66に示すように、メディアSAM133aには、ユーザ登録によって、新たに、ユーザID、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報などのデータに加えて、キーファイルKFの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータC（コンテンツファイルCF）のキーファイルKF、KF₁、並びに所定の検証値（MAC値）が書き込まれる。キーファイルKFの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータC（コンテンツファイルCF）のキーファイルKF、KF₁、並びに所定の検証値（MAC値）は、記録用鍵データKSTRによって暗号化されている。

【0286】＜メディアSAMの第2形態＞図71は、メディアSAM133bの回路モジュールを説明するための図である。図71に示すように、メディアSAM133bは、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、ハッシュ関数モジュール1209、

（真性）乱数発生器1210を有する耐タンパ性のハ

ドウェア（Tamper Registant H/W）である。すなわち、メディアSAM133bは、図66に示すメディアSAM133aから、共通鍵暗号モジュール1208を除いた構成をしている。

【0287】メディアSAM133bの公開鍵暗号モジュール1207は、（1）：図62に示すSAM1051およびドライブCPU1003等と間の相互認証、（2）メディアSAM133の署名データの作成、署名データ（EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ）の検証、（3）：転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアSAM133aの公開鍵暗号モジュール1207とは異なり、（4）：相互認証によって得たセッション鍵データKsesの鍵共有は行わない。鍵の共有を行わないのは、共通鍵暗号モジュール1208を有していないためである。また、メディアSAM133bの公開鍵暗号モジュール1207は、公開鍵暗号方式を用いて、さらにキーファイルKF、KF₁などのデータの暗号化および復号を行う。

【0288】＜メディアSAMの第3形態＞図72は、メディアSAM133cの回路モジュールを説明するための図である。図72に示すように、メディアSAM133cは、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、（真性）乱数発生器1210を有する耐タンパ性のハードウェア（Tamper Registant H/W）である。すなわち、メディアSAM133cは、図66に示すメディアSAM133aから、共通鍵暗号モジュール1208およびハッシュ関数モジュール1209を除いた構成をしている。メディアSAM133cの公開鍵暗号モジュール1207は、（1）：図62に示すSAM1051およびドライブCPU1003等と間の相互認証、（2）メディアSAM133の署名データの作成、（3）：転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアSAM133aの公開鍵暗号モジュール1207とは異なり、署名データの検証および（4）：相互認証によって得たセッション鍵データKsesの鍵共有は行わない。署名データの検証を行わないのは、ハッシュ関数モジュール1209を有していないためである。また、メディアSAM133cの公開鍵暗号モジュール1207は、公開鍵暗号方式を用いて、キーファイルKF、KF₁などのデータの暗号化および復号を行う。この場合に、メディアSAM133cは、署名データの検証を行わないため、SAM1051から公開鍵データKcp.P、Kesc.P（第2実施形態の場合には、さらにサービスプロバイダ310の公開鍵データKsp.P）を受ける。

【0289】＜メディアSAMの第4形態＞図73は、

メディアSAM133dの回路モジュールを説明するための図である。図73に示すように、メディアSAM133dは、CPU1200、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、(真性)乱数発生器1210を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアSAM133cは、図66に示すメディアSAM133aから、DMA1201、共通鍵暗号モジュール1208およびハッシュ関数モジュール1209を除いた構成をしている。メディアSAM133dの公開鍵暗号モジュール1207は、基本的に、前述したメディアSAM133cの公開鍵暗号モジュール1207と同じ機能を有している。メディアSAM133dは、DMA1201を有していないため、マスクROM1204、不揮発性メモリ1205および作業用RAM1206に対してのアクセス制御はCPU1200によって行われる。

【0290】<メディアSAMの第5形態>図74は、メディアSAM133eの回路モジュールを説明するための図である。図74に示すように、メディアSAM133eは、セキュアメモリ133ea、ホストCPU810および耐タンパ性ソフトウェア1130を用いて実現される。セキュアメモリ133eaは、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207および(真性)乱数発生器1210を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。セキュアメモリ133ea内の各モジュールは、同一符号のメディアSAM133dのモジュールと同じである。

【0291】すなわち、セキュアメモリ133eaは、図73に示すメディアSAM133dから、CPU1200を除いた構成をしている。SAM105eでは、ホストCPU810において、耐タンパ性ソフトウェア1250を実行することで、図73に示すCPU1200と同じ機能を実現する。耐タンパ性ソフトウェア1250は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

【0292】<メディアSAMの第6形態>図75は、メディアSAM133fの回路モジュールを説明するための図である。図75に示すように、メディアSAM133fは、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206および公開鍵暗号モジュール1207を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアSAM133fは、図72に示すメディアSAM133cから、乱数生成器1210を除いた構成をしている。メ

ディアSAM133fの公開鍵暗号モジュール1207は、(2)メディアSAM133の署名データの作成、(3):転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアSAM133aの公開鍵暗号モジュール1207とは異なり、署名データの検証、相互認証および(4):相互認証によって得たセッション鍵データKsesの鍵共有は行わない。この場合に、メディア・ドラブSAM260からメディアSAM133fの認証は行われるが、メディアSAM133fが乱数生成器1210を有していないため、メディアSAM133fからメディア・ドラブSAM260の認証は行わない。

【0293】<メディアSAMの第7形態>図76は、メディアSAM133gの回路モジュールを説明するための図である。図76に示すように、メディアSAM133gは、セキュアメモリ133ga、ホストCPU810および耐タンパ性ソフトウェア1260を用いて実現される。図76に示すように、セキュアメモリ133gaは、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206および公開鍵暗号モジュール1207を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアSAM133gaは、図75に示すメディアSAM133fから、CPU1200およびDMA1201を除いた構成をしている。メディアSAM133gの公開鍵暗号モジュール1207の機能は、基本的に前述したメディアSAM133fの公開鍵暗号モジュール1207と同じである。SAM105gでは、ホストCPU810において、耐タンパ性ソフトウェア1260を実行することで、図75に示すCPU1200と同じ機能を実現する。耐タンパ性ソフトウェア1260は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

【0294】<AV圧縮・伸長用SAM163>AV圧縮・伸長用SAM163は、例えば、図22を用いて説明した機能を実現する。図77は、AV圧縮・伸長用SAM163の回路モジュールを説明するための図である。図77に示すように、AV圧縮・伸長用SAM163は、CPU/DSP1300、DMA1301、マスクROM1304、不揮発性メモリ1305、作業用RAM1306、共通鍵暗号モジュール1308、(真性)乱数発生器1310、圧縮・伸長モジュール1320、電子透かし情報付加・検出モジュール1321および情報半開示制御モジュール1322を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0295】CPU/DSP1300は、例えば、図62に示すSAM105iからの命令に応じて、マスクROM1304および不揮発性メモリ1305に記憶されたプログラムを実行し、AV圧縮・伸長用SAM163

内の各回路モジュールを統括的に制御する。DMA1301は、CPU/DSP1300からの命令に応じて、マスクROM1304、不揮発性メモリ1305、作業用RAM1306に対してのアクセスを統括的に制御する。マスクROM1304には、AV圧縮・伸長用SAM163の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムや、AV圧縮・伸長用SAM163の識別子であるAVSAM_IDなどの改変しないデータが製造時に記憶される。不揮発性メモリ1305は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用RAM1306は、SAM1051から入力したキーファイルKFなどを記憶する。

【0296】共通鍵暗号モジュール1308は、SAM1051との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データKsesを用いたコンテンツデータなどの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1308は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1305に記憶した共通鍵暗号プログラムをCPU/DSP1300において実行して実現してもよい(S/W IP Solution)。また、共通鍵暗号モジュール1308は、権利処理用のSAMから入力したコンテンツ鍵データKcを用いて、コンテンツデータの復号を行う。乱数発生器1110は、例えば、SAM1051との間の相互認証処理を行う際に用いられる。

【0297】圧縮・伸長モジュール1320は、例えば、図22に示す伸長部223の機能を実現し、図62に示すダウンロードメモリ167およびショックブルーフメモリ1004から入力したコンテンツデータの伸長処理と、A/D変換器から入力したコンテンツデータの圧縮処理とを行う。

【0298】電子透かし情報添付・検出モジュール1321は、図22に示す電子透かし情報処理部224の機能を実現し、例えば、圧縮・伸長モジュール1320の処理対象となるコンテンツデータに対して所定の電子透かし情報を埋め込むと共に、当該コンテンツデータに埋め込まれた電子透かし情報を検出し、圧縮・伸長モジュール1320による処理の適否を判断する。

【0299】情報半開示制御モジュール1322は、図22に示す半開示処理部225の機能を実現し、必要に応じて、コンテンツデータを半開示状態で再生する。

【0300】なお、AV圧縮伸長SAM163として、例えば、コンテンツファイルCFに格納された図3に示すA/V伸長用ソフトウェアSoftwareおよび電子透かし情報モジュールWMを用いて処理を行う場合には、図78に示すように、図77に示す構成から圧縮・伸長モジュール1320および電子透かし情報添付・検出モジュール1321を除いた構成にすることができる。このようにすることで、AV圧縮伸長用SAM163におい

て、コンテンツプロバイダ101の要求に応じた任意の伸長処理および電子透かし処理を行うことができる。

【0301】<メディア・ドラブSAM260の第1形態>図79は、メディア・ドラブSAM260aの回路モジュールを説明するための図である。図79に示すように、メディア・ドラブSAM260aは、CPU1400、DMA1401、マスクROM1404、不揮発性メモリ1405、作業用RAM1406、共通鍵暗号モジュール1408、ハッシュ関数モジュール1409、(真性)乱数発生器1410、エンコーダ・デコーダモジュール1420、記録用鍵データ生成モジュール1430およびメディア・ユニークID生成モジュール1440を有する耐タンパ性のハードウェア(Tamper Resistant H/W)である。

【0302】CPU1400は、例えば、図62に示すドライブCPU1003からの命令に応じて、マスクROM1404および不揮発性メモリ1405に記憶されたプログラムを実行し、メディア・ドラブSAM260a内の各回路モジュールを統括的に制御する。DMA1401は、CPU1400からの命令に応じて、マスクROM1404、不揮発性メモリ1405、作業用RAM1406に対してのアクセスを統括的に制御する。マスクROM1404には、メディア・ドラブSAM260aの初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムや、メディア・ドラブSAM260aの識別子であるMDSAM_IDなどの改変しないデータが製造時に記憶される。不揮発性メモリ1405は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用RAM1406は、種々の処理を行う際の作業用メモリとして用いられる。

【0303】共通鍵暗号モジュール1408は、メディアSAM133およびAV圧縮・伸長用SAM163との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データKsesを用いたコンテンツファイルCFおよびキーファイルKFなどの暗号化および復号、並びに記録用鍵データKstrを用いたコンテンツ鍵データKcの暗号化などを行う際に用いられる。また、共通鍵暗号モジュール1408は、共通鍵データと署名の対象となるデータのハッシュ値を用いて、署名データの検証および作成を行う。共通鍵暗号モジュール1408は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1405に記憶した共通鍵暗号プログラムをCPU1400において実行して実現してもよい(S/W IP Solution)。なお、記録用鍵データKstrを用いたコンテンツ鍵データKcの暗号化は、メディア・ドラブSAM260の共通鍵暗号モジュール1408およびメディアSAM133の何れで行ってもよい。ハッシュ関数モジュール1409は、署名データの検証、並びに署名データを作成する対象となるデータのハッシュ

値を生成する際に用いられる。乱数発生器1410は、例えば、メディアSAM133との間の相互認証処理を行う際に用いられる。

【0304】エンコーダ・デコーダモジュール1420は、記録媒体130のROM領域あるいはRAM領域に対して、コンテンツデータのアクセスを行う際に、当該コンテンツデータのエンコード処理、デコード処理、ECC(Error Correction Code)処理、変調処理、復調処理、セクタライズ処理およびデセクタライズ処理などを行う。

【0305】記録用鍵データ生成モジュール1430は、メディア・ユニークID生成モジュール1440が生成したメディア・ユニークIDを用いて、各メディアにユニークな記録用鍵データKSTRを生成する。

【0306】メディア・ユニークID生成モジュール1440は、メディア・ドライブSAM260で生成したドライブIDと、メディアSAM133のメディアSAM-IDとから、各記録媒体(メディア)にユニークなメディア・ユニークIDを生成する。

【0307】また、図80に示すように、図79に示すメディア・ドライブSAM260aにおいて共通鍵暗号モジュール1408の代わりに公開鍵暗号モジュール1407を用いた構成のメディア・ドライブSAM260c用いてもよい。

【0308】<メディア・ドライブSAM260の第2形態>図81は、メディア・ドライブSAM260bを説明するための図である。図81では、メディア・ドライブSAM260aの構成要素と同じものには、図78と同じ符号を付している。図81に示すように、メディア・ドライブSAM260bは、セキュアメモリ260ba、図62に示すドライブCPU1003、耐タンパ性ソフトウェア1450を用いて実現される。メディア・ドライブSAM260bでは、ドライブCPU1003において、耐タンパ性ソフトウェア1450を実行することで、図80に示すCPU1400と同じ機能を実現する。耐タンパ性ソフトウェア1450は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。セキュアメモリ260baは、マスクROM1404、不揮発性メモリ1405、作業用RAM1406、共通鍵暗号モジュール1408、ハッシュ関数モジュール1409、(真性)乱数発生器1410、エンコーダ・デコーダモジュール1420、記録用鍵データ生成モジュール1430およびメディア・ユニークID生成モジュール1440を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【0309】また、図82示すように、図81に示すメディア・ドライブSAM260bにおいて共通鍵暗号モジュール1408の代わりに公開鍵暗号モジュール1407を用いた構成のメディア・ドライブSAM260d用

いてもよい。

【0310】以下、図1に示すEMDシステム100の全体動作について説明する。図83は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1: EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データKCP、Pの公開鍵証明書CERCPをコンテンツプロバイダ101に送信する。また、EMDサービスセンタ102は、SAM1051~1054が所定の登録処理を経た後に、SAM1051~1054の公開鍵データKSA1,P~KSA4,Pの公開鍵証明書CERCP1~CERCP4をSAM1051~1054に送信する。また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の3カ月分のライセンス鍵データKD1~KD3をユーザホームネットワーク103のSAM1051~1054に送信する。このように、EMDシステム100では、ライセンス鍵データKD1~KD3を予めSAM1051~1054に配給しているため、SAM1051~1054とEMDサービスセンタ102との間がオフラインの状態でも、SAM1051~1054においてコンテンツプロバイダ101から配給されたセキュアコンテンツ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM1051~1054とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。なお、利用制御状態データ166は、原則として、リアルタイムで、SAM1051~1054からEMDサービスセンタ102に送信される。

【0311】ステップS2: コンテンツプロバイダ101は、EMDサービスセンタ102との間で相互認証を行った後に、権利書データ106およびコンテンツ鍵データKcをEMDサービスセンタ102に登録して権威化する。また、EMDサービスセンタ102は、6カ月のキーファイルKFを作成し、これをコンテンツプロバイダ101に送信する。

【0312】ステップS3: コンテンツプロバイダ101は、図3(A),(B)に示すコンテンツファイルCFおよびその署名データSIG6,CPと、キーファイルKFおよびその署名データSIG7,CPとを作成し、これらと図3(C)に示す公開鍵証明書データCERCPおよびその署名データSIG1,ESCとを格納したセキュアコンテンツ104を、オンラインおよび/またはオフラインで、ユーザホームネットワーク103のSAM1051~1054に配給する。オンラインの場合には、コンテ

ンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ104がコンテンツプロバイダ101からユーザホームネットワーク103に配送される。また、オフラインの場合には、ROM型あるいはRAM型の記録媒体に記録された状態で、セキュアコンテナ104が、コンテンツプロバイダ101からユーザホームネットワーク103に配送される。

【0313】ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、コンテンツプロバイダ101から配給を受けたセキュアコンテナ104内の署名データSIG_{6,CP}, SIG_{7,CP}, SIG_{K1,ESG}を検証して、コンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認した後、対応する期間のライセンス鍵データKD₁～KD₆を用いてキーファイルKFを復号する。

【0314】ステップS5：SAM105₁～SAM105₄において、ユーザによる図22に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。このとき、図30に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

【0315】ステップS6：SAM105₁～SAM105₄の図30に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0316】ステップS7：EMDサービスセンタ102は、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG₉₉を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0317】ステップS8：決済機関91において、署名データSIG₉₉の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0318】以上説明したように、EMDシステム100では、図3に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105₁～105₄内で行う。また、キーファイルKFに格納され

たコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₃を用いて暗号化されており、配信鍵データKD₁～KD₃を保持しているSAM105₁～105₄内でのみ復号される。そして、SAM105₁～105₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

【0319】また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁～105₄におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

【0320】また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0321】図84は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。図84に示すように、マルチプロセッサシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを転送するプロトコルとして例えば1394シリアルバス・インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

【0322】第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0323】図85は、本実施形態のEMDシステム3

00の構成図である。図85に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。コンテンツプロバイダ301、EMDサービスセンタ302、SAM3051~3054およびサービスプロバイダ310は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM5051~5054に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。また、ユーザホームネットワーク303は、ネットワーク機器3601およびAV機器3602~3604を有している。ネットワーク機器3601はSAM3051およびCAモジュール311を内蔵しており、AV機器3602~3604はそれぞれSAM3052~3054を内蔵している。ここで、SAM3051~3054は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM1051~1054と同じである。

【0324】先ず、EMDシステム300の概要について説明する。EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106およびコンテンツ鍵データKcを、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106およびコンテンツ鍵データKcは、EMDサービスセンタ302に登録されて権威化（認証）される。

【0325】また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。そして、コンテンツプロバイダ301は、コンテンツファイルCF、

キーファイルKFおよび自らの署名データとを格納した図3に示すセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ310に供給する。また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0326】サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104の作成者および送信者の確認する。次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対する価格（SRP）に、自らが行ったオーサリングなどのサービスに対する価格を加算した価格を示すプライスタグデータ（PT：本発明の価格データ）312を作成する。そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対する自らの秘密鍵データKsp.sによる署名データとを格納したセキュアコンテナ304を作成する。このとき、キーファイルKFは、ライセンス鍵データKD1~KD6によって暗号化されており、サービスプロバイダ310は当該ライセンス鍵データKD1~KD6を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

【0327】サービスプロバイダ310は、オンラインおよび/またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。このとき、オフラインの場合には、セキュアコンテナ304はROM型の記録媒体などに記録されてSAM3051~3054にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データKsesを用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データKsesを用いて復号した後に、SAM3051~3054に転送する。この場合に、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を送信する通信プロトコルとして、デジタル放送であればMHPEG (Multimedia and Hypertext Information Coding Experts Group) プロトコルが用いられ、インターネットであればXML/SMIL/HTML (Hyper Text Markup Language) が用いられ、これらの通信プロトコル内に、セキュアコンテナ3

04が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。従って、通信プロトコルとセキュアコンテナ304との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ304のフォーマットを柔軟に設定できる。

【0328】次に、SAM3051～3054において、セキュアコンテナ304内に格納された署名データを検証して、セキュアコンテナ304に格納されたコンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認する。そして、SAM3051～3054において、当該正当性が確認されると、EMDサービスセンタ302から配給された対応する期間のライセンス鍵データKD1～KD3を用いてキーファイルKFを復号する。SAM3051～3054に供給されたセキュアコンテナ304は、ネットワーク機器3601およびAV機器3602～3604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM3051～3054は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。また、SAM3051～3054は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御データ（UCS:Usage control state Data）166をEMDサービスセンタ302に送信する。

【0329】EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

【0330】本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ

301の権利書データ106、コンテンツ鍵データKcおよびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。また、EMDサービスセンタ302は、例えば、ライセンス鍵データKD1～KD3などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM3051～SAM3054から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機能を有する。

【0331】以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

【コンテンツプロバイダ301】コンテンツプロバイダ301は、図3に示すセキュアコンテナ104をオンラインあるいはオフラインでサービスプロバイダ310に提供する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。すなわち、コンテンツプロバイダ301は、前述した図17～図19に示す手順でセキュアコンテナ104を作成し、セキュアコンテナ104を、コンテンツプロバイダ用商品配送プロトコルに挿入する。そして、サービスプロバイダ310が、ダウンロードを行って、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ104を取り出す。

【0332】【サービスプロバイダ310】サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を作成し、ユーザホームネットワーク303のネットワーク機器3601およびAV機器3602～3604にセキュアコンテナ304をオンラインおよび/またはオフラインで配給する。サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0333】サービスプロバイダ310は、コンテンツ

プロバイダ301からセキュアコンテナ104の提供を受けると、以下に示す処理を行ってセキュアコンテナ304を作成する。以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図86を参照しながら説明する。図86は、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を配給する処理を説明するためのフローチャートである。

<ステップS86-1>サービスプロバイダ310は、オンラインおよび/またはオフラインで、コンテンツプロバイダ301から図3に示すセキュアコンテナ104の供給を受け、これを格納する。このとき、オンラインの場合には、コンテンツプロバイダ301とサービスプロバイダ310との間の相互認証によって得られたセッション鍵データKsesを用いて、セキュアコンテナ104を復号する。

<ステップS86-2>サービスプロバイダ310は、セキュアコンテナ104の図3(C)に示す署名データSIG1.escを、EMDサービスセンタ302の公開鍵データKesc.pを用いて検証し、その正当性が認められた後に、図3(C)に示す公開鍵証明書データCERcpから公開鍵データKcp.pを取り出す。次に、サービスプロバイダ310は、当該取り出した公開鍵データKcp.pを用いて、セキュアコンテナ104の図3(A),

(B)に示す署名データSIG6.cp, SIG7.cpの検証、すなわちコンテンツファイルCFの作成者および送信者と、キーファイルKFの送信者との正当性の検証を行う。また、サービスプロバイダ310は、公開鍵データKesc.pを用いて、図3(B)に示すキーファイルKFに格納された署名データSIGk1.escの検証、すなわちキーファイルKFの作成者の正当性の検証を行う。このとき、署名データSIGk1.escの検証は、キーファイルKFがEMDサービスセンタ302に登録されているか否かの検証も兼ねている。

【0334】<ステップS86-3>サービスプロバイダ310は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成する。また、サービスプロバイダ310は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データKsp.pを用いて、署名データSIG62.sp, SIG63.sp, SIG64.spを作成する。ここで、署名データSIG62.spはコンテンツファイルCFの送信者の正当性を検証するために用いられ、署名データSIG63.spはキーファイルKFの送信者の正当性を検証するために用いられ、署名データSIG64.sp

はプライスタグデータ312の作成者および送信者の正当性を検証するために用いられる。

【0335】次に、サービスプロバイダ310は、図87(A)~(D)に示すように、コンテンツファイルCFおよびその署名データSIG6.cp, SIG62.spと、キーファイルKFおよびその署名データSIG7.cp, SIG63.escと、プライスタグデータ312およびその署名データSIG64.spと、公開鍵証明書データCERcpおよびその署名データSIG1.escと、公開鍵証明書データCERcpおよびその署名データSIG1.escとを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベースに格納する。セキュアコンテナデータベースに格納されたセキュアコンテナ304は、例えば、コンテンツIDなどを用いてサービスプロバイダ310によって一元的に管理される。なお、図87(A)は、コンテンツデータCを伸長するAV圧縮伸長用装置として、DSP(Digital Signal Processor)を用いた場合のコンテンツファイルCFの構成である。当該DSPでは、セキュアコンテナ304内のA/V伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ104内のコンテンツデータCの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ301は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。AV圧縮伸長用装置としてA/V伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルCF内にA/V伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0336】<ステップS86-4>サービスプロバイダ310は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベースから読み出す。このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

【0337】また、セキュアコンテナ304は、デジタル放送で送信される場合には、MHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML(Hyper TextMarkup Language)プロトコルが用いられる。このとき、セキュアコンテナ304内のコンテンツファイルCFおよびキーファイルKFなどは、MHEGおよびHTMLのプロトコ

ルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ310とユーザホームネットワーク303との間で採用される通信プロトコル内の所定の階層に格納される。

【0338】例えば、セキュアコンテナ304をデジタル放送で送信する場合には、図88に示すように、コンテンツファイルCFが、MHEGオブジェクト(Object)内のMHEGコンテンツデータとして格納される。また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES(Packetized Elementary Stream)-Videoに格納され、音声である場合にはPES-Audioに格納され、静止画である場合にはPrivate-Dataに格納される。また、図89に示すように、キーファイルKF、プライスタグデータ312および公開鍵証明書データCERcp, CERspは、トランスポート層プロトコルのTS Packet内のECM(Entitlement Control Message)に格納される。ここで、コンテンツファイルCF、キーファイルKF、プライスタグデータ312および公開鍵証明書データCERcp, CERspは、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSD1によって相互間のリンクが確立されている。

【0339】次に、サービスプロバイダ310は、セキュアコンテナ304を、オフラインおよび/またはオンラインでユーザホームネットワーク303に供給する。サービスプロバイダ310は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器3601に配信する場合には、相互認証後に、セッション鍵データKsesを用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器3601に配信する。

【0340】なお、サービスプロバイダ310は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データKscrを用いて暗号化する。また、スクランブル鍵データKscrをワーク鍵データKwを暗号化し、ワーク鍵データKwをマスタ鍵データKmを用いて暗号化する。そして、サービスプロバイダ310は、セキュアコンテナ304と共に、スクランブル鍵データKscrおよびワーク鍵データKwを、衛星を介してユーザホームネットワーク303に送信する。また、例えば、マスタ鍵データKmを、ICカードなどに記憶してオフラインでユーザホームネットワーク303に配給する。

【0341】また、サービスプロバイダ310は、ユーザホームネットワーク303から、当該サービスプロバイダ310が配給したコンテンツデータCに関してのSP用購入履歴データ309を受信すると、これを格納する。サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購入履歴データ309を参照する。また、サービスプロバイダ310は、SP用購入履

歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM3051~3054のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク303のCAモジュール311に送信する。

【0342】また、サービスプロバイダ310の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。

【0343】また、サービスプロバイダ310は、EMDサービスセンタ302にプライスタグデータ312を登録して権威化して。

【0344】[EMDサービスセンタ302] EMDサービスセンタ302は、前述したように、認証局(CA:CertificateAuthority)、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。図90は、EMDサービスセンタ302の主な機能を示す図である。図90に示すように、EMDサービスセンタ302は、主に、ライセンス鍵データをコンテンツプロバイダ301およびSAM3051~3054に供給する処理と、公開鍵証明書データCERcp, CERsp, CERSAN1~CERSAN4の発行処理と、キーファイルKFの発行処理、利用履歴データ308に基づいた決済処理(利益分配処理)とを行う。ここで、ライセンス鍵データの供給処理と、公開鍵証明書データCERcp, CERSAN1~CERSAN4の発行処理と、キーファイルKFの生成処理とは、第1実施形態のEMDサービスセンタ102と同じである。

【0345】EMDサービスセンタ302は、EMDサービスセンタ102とは異なり、さらにサービスプロバイダ310の公開鍵証明書データCERspの発行処理を行う。また、EMDサービスセンタ302は、利用履歴データ308に基づいて、SAM3051~3054におけるコンテンツデータCの購入によって支払われた利益をコンテンツプロバイダ301およびサービスプロバイダ310の関係者に分配する利益分配処理を行う。ここで、利用履歴データ308の内容は、例えば図21に示される。

【0346】また、EMDサービスセンタ302は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM3051~3054のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM3051~3054に送信する。

【0347】[ユーザホームネットワーク303] ユーザホームネットワーク303は、図85に示すように、ネットワーク機器3601およびA/V機器3602~

3604を有している。ネットワーク機器3601は、CAモジュール311およびSAM3051を内蔵している。また、AV機器3602～3604は、それぞれSAM3052～3054を内蔵している。SAM3051～3054の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続されている。なお、AV機器3602～3604は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器3601のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0348】以下、ネットワーク機器3601について説明する。図91は、ネットワーク機器3601の構成図である。図91に示すように、ネットワーク機器3601は、通信モジュール162、CAモジュール311、復号モジュール905、SAM3051、AV圧縮・伸長用SAM163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。図91において、図22と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

【0349】通信モジュール162は、サービスプロバイダ310との間の通信処理を行なう。具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテンツ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310から電話回線などを介して受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0350】図92は、CAモジュール311および復号モジュール905の機能ブロック図である。図92に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データKsesを生成し、これを暗号化・復号部908に出力する。

【0351】記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データKmを記憶する。

【0352】暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクラ

ンブル鍵データKscrおよびワーク鍵データKwを入力し、記憶部907から読み出したマスタ鍵データKmを用いてワーク鍵データKwを復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データKwを用いてスクランブル鍵データKscrを復号し、当該復号したスクランブル鍵データKscrを復号部910に出力する。また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データKsesを用いて復号して復号モジュール905のセキュアコンテンツ選択部911に出力する。また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データKsesを用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

【0353】SP用購入履歴データ生成部909は、図91に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータCの購入操作に応じた操作信号S165、またはSAM3051からの利用制御データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履歴データ309を生成し、これを暗号化・復号部908に出力する。SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0354】なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0355】復号モジュール905は、復号部910およびセキュアコンテンツ選択部911を有する。復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテンツ304、スクランブル鍵データKscrおよびワーク鍵データKwを入力する。そして、復号部910は、暗号化されたスクランブル鍵データKscrおよびワーク鍵データKwをCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データKscrを入力する。そして、復号部910は、暗号化されたセキュアコンテンツ304を、スクランブル鍵データKscrを用いて復号した後に、セキュアコンテンツ選択部911に出力する。

【0356】なお、セキュアコンテンツ304が、MPEG2

Transport Stream 方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet 内のECM(Entitlement Control Message)からスクランブル鍵データK_{SCR}を取り出し、EMM(Entitlement Management Message)からワーク鍵データK_Wを取り出す。ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ(視聴者)毎に異なる個別視聴契約情報などが含まれている。

【0357】セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM3051に出力する。

【0358】次に、SAM3051について説明する。なお、SAM3051は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図22～図61などを用いて前述した第1実施形態のSAM1051と基本的に行なう機能および構造を有している。している。SAM3051～3054は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0359】また、図62に示す構成はユーザホームネットワーク303内の機器においても適用可能である。また、図63～図82を用いて説明した権利処理用のSAM、メディアSAM133、AV圧縮・伸長用SAM163およびメディア・ドラブSAM260の構成は、ユーザホームネットワーク303内の機器で用いられる各種のSAMにも適用される。また、SAM3052～3054は、SAM3051と基本的に同じ機能を有

【0360】以下、SAM3051の機能について詳細に説明する。図93は、SAM3051の機能の構成図である。なお、図93には、サービスプロバイダ310からセキュアコンテナ304を入力する際の処理に関連するデータの流れが示されている。図93に示すように、SAM3051は、相互認証部170、暗号化・復号部171、172、173、ダウンロードメモリ管理部182、AV圧縮・伸長用SAM管理部184、EMDサービスセンタ管理部185、利用監視部186、SAM管理部190、記憶部192、メディアSAM管理部197、作業用メモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部589および外部メモリ管理部811を有する。なお、図93に示すSAM3051の所定の機能は、SAM1051の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。図93において、図23等と同じ符号を付した機能ブロックは、第1実施形態で説明

した同一符号の機能ブロックと同じである。ここで、コンテンツプロバイダ管理部180およびダウンロードメモリ管理部182が本発明の入力処理手段に対応し、課金処理部587が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部172が本発明の復号手段に対応し、利用監視部186が本発明の利用制御手段に対応している。また、暗号化・復号部173が本発明の暗号化手段に対応している。また、後述する例えば図91に示すメディア・ドライブSAM管理部855が本発明の記録制御手段に対応している。また、署名処理部189が本発明の署名処理手段に対応している。

【0361】また、図91に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。また、作業用メモリ200には、図94に示すように、コンテンツ鍵データK_c、権利書データ(UCP)106、記憶部192のロック鍵データK_{Loc}、コンテンツプロバイダ301の公開鍵証明書データCER_{Op}、サービスプロバイダ310の公開鍵証明書データCER_{Sp}、利用制御データ(UCS)366、SAMプログラム・ダウンロード・コンテナSDC1～SDC3およびプライスタグデータ312などが記憶される。

【0362】以下、SAM3051の機能ブロックのうち、図93において新たに符号を付した機能ブロックについて説明する。署名処理部589は、記憶部192あるいは作業用メモリ200から読み出したEMDサービスセンタ302の公開鍵データK_{Esc.P}、コンテンツプロバイダ301の公開鍵データK_{Op.P}およびサービスプロバイダ310の公開鍵データK_{Sp.P}を用いて、セキュアコンテナ304内の署名データの検証を行なう。

【0363】課金処理部587は、図95に示すように、図91に示す購入・利用形態決定操作部165からの操作信号S165と、作業用メモリ200から読み出されたプライスタグデータ312とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。なお、プライスタグデータ312は、ユーザがコンテンツデータの購入形態等を決定する際に、所定の出力手段を介してSAM3051の外部に出力され、コンテンツデータの販売価格をユーザに表示等するために用いられる。課金処理部587による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0364】また、課金処理部587は、課金処理において、利用履歴データ308を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。

【0365】また、課金処理部587は、操作信号S165に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ166を生成し、これを作業用メモリ200に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ166には、コンテンツのID、購入形態、買い切り価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0366】なお、決定された購入形態が再生課金である場合には、例えば、SAM305i からサービスプロバイダ310に利用制御データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ308をSAM105i に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0367】また、SAM305i では、図93に示すように、EMDサービスセンタ管理部185を介してEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図91に示す復号モジュール905から入力したセキュアコンテナ304のうち、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304がダウンロードメモリ管理部182に出力される。これにより、SAM305i において、当該SAM305i のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0368】以下、SAM305i 内での処理の流れを説明する。

<ライセンス鍵データの受信時の処理> EMDサービスセンタ302から受信したライセンス鍵データKD1 ~ KD3を記憶部192に格納する際のSAM305i 内での処理の流れは、図28を用いて前述した第1実施形

態のSAM105i の場合と同様である。

【0369】<セキュアコンテナ304をサービスプロバイダ310から入力した時の処理> 次に、セキュアコンテナ304をサービスプロバイダ310から入力する際のSAM305i 内での処理の流れを図96を参照しながら説明する。なお、以下に示す例では、SAM105i において、セキュアコンテナ104を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ104の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップS96-1: 図93に示すSAM305i の相互認証部170とサービスプロバイダ310との間で相互認証を行なう。

ステップS96-2: SAM305i の相互認証部170とダウンロードメモリ167のメディアSAM167aとの間で相互認証を行なう。

【0370】ステップS96-3: サービスプロバイダ310から受信したセキュアコンテナ304を、ダウンロードメモリ167に書き込む。このとき、ステップS96-2で得られたセッション鍵データを用いて、相互認証部170におけるセキュアコンテナ304の暗号化と、メディアSAM167aにおけるセキュアコンテナ304の復号とを行なう。

ステップS96-4: SAM305i は、ステップS96-1で得られたセッション鍵データを用いて、セキュアコンテナ304の復号を行なう。

【0371】ステップS96-5: 署名処理部589は、図87(D)に示す署名データSIG61.ESCの検証を行なった後に、図87(D)に示す公開鍵証明書データCERSP内に格納されたサービスプロバイダ310の公開鍵データKSP.Pを用いて、署名データSIG62.SP, SIG63.SP, SIG64.SPの正当性を検証する。このとき、署名データSIG62.SPが正当であると検証されたときに、コンテンツファイルCFの送信者の正当性が確認される。署名データSIG63.SPが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。署名データSIG64.SPが正当であると検証されたときに、プライスタグデータ312の作成者および送信者の正当性が確認される。

【0372】ステップS96-6: 署名処理部589は、図87(D)に示す署名データSIG1.ESCの検証を行なった後に、図87(C)に示す公開鍵証明書データCERCP内に格納されたコンテンツプロバイダ301の公開鍵データKCP.Pを用いて、署名データSIG6.CP, SIG7.CPの正当性を検証する。このとき、署名データSIG6.CPが正当であると検証されたときに、コンテンツファイルCFの作成者および送信者の正当性が確認される。また、署名データSIG7.CPが正当であると検証されたときに、キーファイルKFの送信者の正

当性が確認される。

【0373】ステップS96-7:署名処理部589は、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて、図87(B)に示すキーファイルKF内の署名データSIG_{K1,ESC}の正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

【0374】ステップS96-8:暗号化・復号部172は、記憶部192から読み出した対応する期間のライセンス鍵データKD₁~KD₃を用いて、図87(B)に示すキーファイルKF内のコンテンツ鍵データK_C、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁~SDC₃を復号し、これらを作業用メモリ200に書き込む。

【0375】<ダウンロードしたセキュアコンテナの購入形態決定処理>ダウンロードしたセキュアコンテナの購入形態決定処理は、基本的に、第1実施形態において、図31を用いて前述したSAM105₁の場合と同じである。当該購入形態決定処理により、後述する図100(C)に示すキーファイルKF₁が作業用メモリ200およびダウンロードメモリ管理部182を介してダウンロードメモリ167に記憶される。

【0376】<コンテンツデータの再生処理>ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCの再生処理は、基本的に、第1実施形態において、図33を用いて説明したSAM105₁の処理と同じである。

【0377】<一の機器の利用制御データ(USC)166を使用して他の機器で再購入を行う場合の処理>先ず、図97に示すように、例えば、ネットワーク機器360₁のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの購入形態を前述したように決定した後に、当該コンテンツファイルCFを格納した新たなセキュアコンテナ304xを生成し、バス191を介して、AV機器360₂のSAM305₂にセキュアコンテナ304xを転送するまでのSAM105₁内での処理の流れを図98および図99を参照しながら説明する。

【0378】図99は、当該処理のフローチャートである。図99に示す処理を行う前提として、前述した購入処理によって、SAM305₁の作業用メモリ200には図100(C)に示すキーファイルKF₁、およびそのハッシュ値H_{K1}が記憶されている。

ステップS99-1:ユーザは、図91および図97に示すに購入・利用形態決定操作部165を操作して、購入形態を既に決定したセキュアコンテナをSAM305₂に転送することを指示する。課金処理部587は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ308を更新する。

【0379】ステップS99-2: SAM305₁は、第1実施形態で前述したSAM登録リストを検証し、セキュアコンテナの転送先のSAM305₂が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS96-3以降の処理を行う。また、SAM105₁は、SAM105₂がホームネットワーク内のSAMであるか否かの検証も行う。

【0380】ステップS99-3:相互認証部170は、SAM305₂との間で相互認証を行って得たセッション鍵データK_{SES}を共有する。

【0381】ステップS99-4: SAM管理部190は、ダウンロードメモリ211から図87(A)に示すコンテンツファイルCFおよび署名データSIG_{G6,CP}, SIG_{G6,SP}を読み出し、これについてのSAM105₁の秘密鍵データK_{SAM1}を用いた署名データSIG_{41,SAM1}を署名処理部189に作成させる。

【0382】ステップS99-5: SAM管理部190は、ダウンロードメモリ211から図87(B)に示すキーファイルKFおよび署名データSIG_{7,CP}, SIG_{63,SP}を読み出し、これについてのSAM305₁の秘密鍵データK_{SAM1}を用いた署名データSIG_{42,SAM1}を署名処理部589に作成させる。

【0383】ステップS99-6: SAM管理部190は、図100に示すセキュアコンテナ304xを作成する。

ステップS99-7:暗号化・復号部171において、ステップS96-3で得たセッション鍵データK_{SES}を用いて、図100に示すセキュアコンテナ304xが暗号化される。

【0384】ステップS99-8: SAM管理部190は、セキュアコンテナ304xを図97に示すAV機器360₂のSAM305₂に出力する。このとき、SAM305₁とSAM305₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0385】以下、図97に示すように、SAM305₁から入力した図100に示すセキュアコンテナ304xを、RAM型などの記録媒体(メディア)130₄に書き込む際のSAM305₂内での処理の流れを図101、図102および図103を参照して説明する。図102および図103は、当該処理を示すフローチャートである。ここで、RAM型の記録媒体130₄は、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

【0386】ステップS102-1: SAM305₂は、SAM登録リストを検証し、セキュアコンテナの転送元のSAM305₁が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS99-2以降の処理を行う。また、

SAM3052は、SAM3051がホームネットワーク内のSAMであるか否かの検証も行う。

【0387】ステップS102-2：前述したステップS99-3に対応する処理として、SAM3052は、SAM3051との間で相互認証を行って得たセッション鍵データKsesを共有する。

ステップS102-3：SAM3052のSAM管理部190は、図97に示すように、ネットワーク機器3601のSAM3051からセキュアコンテナ304xを入力する。

ステップS102-4：暗号化・復号部171は、ステップS99-2で共有したセッション鍵データKsesを用いて、SAM管理部190を介して入力したセキュアコンテナ304xを復号する。

【0388】ステップS102-5：セッション鍵データKsesを用いて復号されたセキュアコンテナ304x内のコンテンツファイルCFが、図97に示すメディア・ドライブSAM260におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のRAM領域134に記録される。

【0389】ステップS102-6：セッション鍵データKsesを用いて復号されたセキュアコンテナ304x内の署名データSIG6.cp, SIG62.SP, SIG41.SAM1と、キーファイルKFおよびその署名データSIG7.cp, SIG63.SP, SIG42.SAM1と、キーファイルKF1およびそのハッシュ値HK1と、公開鍵署名データCERspおよびその署名データSIG61.ESCと、公開鍵署名データCERcpおよびその署名データSIG1.ESCと、公開鍵署名データCERsam1およびその署名データSIG22.ESCとが、作業用メモリ200に書き込まれる。

【0390】ステップS102-7：署名処理部589において、作業用メモリ200から読み出された署名データSIG61.ESC, SIG1.ESC, SIG22.ESCが、記憶部192から読み出した公開鍵データKesc.pを用いて検証され、公開鍵証明書データCERsp, CERcp, CERsam1の正当性が確認される。そして、署名処理部589において、公開鍵証明書データCERcpに格納された公開鍵データKcp.pを用いて、署名データSIG6.cpの正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。署名処理部589において、公開鍵証明書データCERspに格納された公開鍵データKsp.pを用いて、署名データSIG62.cpの正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。また、署名処理部189において、公開鍵証明書データCERsam1に格納された公開鍵データKsam1.pを用いて、署名データSIG41.SAM1の正当性が検証され、コンテンツファイルCFの送信者の正当性が

確認される。

【0391】ステップS102-8：署名処理部589において、公開鍵証明書データCERcp, CERsp, CERsam1に格納された公開鍵データKcp.p, Ksp.p, Ksam1.pを用いて、作業用メモリ200に記憶されている署名データSIG7.cp, SIG63.SP, SIG42.SAM1の正当性を検証する。そして、署名データSIG7.cp, SIG63.SP, SIG42.SAM1が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0392】ステップS102-9：署名処理部589において、記憶部192から読み出した公開鍵データKesc.pを用いて、図100(B)のキーファイルKFに格納された署名データSIGk1.ESCの検証が行われる。そして、署名データSIGk1.ESCが正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

【0393】ステップS102-10：署名処理部189は、ハッシュ値HK1の正当性を検証し、キーファイルKF1の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルKF1の作成者と送信元とが同じ場合を述べたが、キーファイルKF1の作成者と送信元とが異なる場合には、キーファイルKF1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0394】ステップS102-11：利用監視部186は、ステップS99-10で復号されたキーファイルKF1に格納された利用制御データ166を用いて、以後のコンテンツデータCの購入・利用形態を制御する。

【0395】ステップS102-12：ユーザは、購入・利用形態決定操作部165を操作して購入形態を決定し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

ステップS102-13：課金処理部587は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ308を更新する。また、課金処理部587は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ166を更新する。

【0396】ステップS102-14：暗号化・復号部173は、記憶部192から読み出した記録用鍵データKstr、メディア鍵データKmedおよび購入者鍵データKpinを順に用いて、ステップS99-12で生成された利用制御データ166を暗号化してメディア・ドライブSAM管理部855に出力する。

ステップS102-15：メディア・ドライブSAM管理部855は、新たな利用制御データ166を格納したキーファイルKF1を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処

理、変調処理および同期処理を経て、RAM型の記録媒体1304のセキュアRAM領域132に記録する。
ステップS102-16: キーファイルKFが作業用メモリ200から読み出され、メディア・ドライブSAM管理部855を介して、図97に示すメディア・ドライブSAM260によってRAM型の記録媒体1304のセキュアRAM領域132に書き込まれる。

【0397】なお、SAM3051におけるROM型の記録媒体のコンテンツデータの購入形態決定処理、ROM型の記録媒体のコンテンツデータの購入形態を決定した後、RAM型の記録媒体に書き込む場合の処理は、サービスプロバイダ310において秘密鍵データKsp,pを用いて付けられた署名データSIGspの検証処理を行う点を除いて、前述した第1実施形態のSAM1051における処理と同じである。また、SAM3051の実現方法も、前述した第1実施形態で説明したSAM1051の実現方法と同じである。また、ユーザホームネットワーク303に用いられる機器においても、第1実施形態で説明した図62に示す構成は同様に適用される。また、この場合に、SAM3051、AV圧縮・伸長用SAM163、メディア・ドライブSAM260およびメディアSAM133の回路モジュールとして、図63～図82を用いて説明した構成が同様に適用される。また、図57～図61を用いて説明したセキュア機能も、コンテンツプロバイダ101がサービスプロバイダ310に置き換える点を除いて、EMDシステム300でも同様に適用される。

【0398】以下、ユーザホームネットワーク303における各種の機器の接続形態等を再び説明する。図104は、ユーザホームネットワーク303における機器の接続形態の一例を説明するための図である。ここでは、図104に示すように、ユーザホームネットワーク303内でネットワーク機器3601、AV機器3602、3603がIEEE1394シリアルバス191を介して接続されている場合を説明する。ネットワーク機器3601は、外部メモリ201、SAM3051、CAMジュール311、AV圧縮・伸長用SAM163およびダウンロードメモリ167を有する。CAMジュール311は、公衆回線などのネットワークを介して、サービスプロバイダ310と通信を行う。また、SAM3051は、公衆回線などのネットワークを介して、EMDサービスセンタ302と通信を行う。ダウンロードメモリ167としては、メディアSAM167aを備えたメモリスティック、あるいはHDDなどが用いられる。ダウンロードメモリ167には、サービスプロバイダ310からダウンロードしたセキュアコンテンツ304などが記憶される。各機器には、ATRAC3やMPEGなどの各種の圧縮・伸長方式にそれぞれ対応した複数のAV圧縮・伸長用SAM163が内蔵されている。SAM3051は、接触方式あるいは非接触方式のICカード11

41と通信を行うことが可能である。ICカード1141は、ユーザIDなどの各種のデータが記憶しており、SAM3051においてユーザ認証を行う場合などに用いられる。

【0399】AV機器3602は、例えば、ストレージ機器であり、SAM3051と3052との間で所定の処理を経て、IEEE1394シリアルバス191を介してネットワーク機器3601から入力したセキュアコンテンツを記録媒体130に記録する。また、AV機器3603も同様に、例えば、ストレージ機器であり、SAM3052と3053との間で所定の処理を経て、IEEE1394シリアルバス191を介してAV機器3602から入力したセキュアコンテンツを記録媒体130に記録する。

【0400】なお、図104に示す例では、記録媒体130にメディアSAM133が搭載されている場合を例示したが、例えば、記録媒体130のメディアSAM133が搭載されていない場合には、図104に点線で示したように、メディア・ドライブSAM260を用いて、SAM3052、3053との間の認証が行われる。

【0401】次に、図85に示すEMDシステム300の全体動作について説明する。図105および図106は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を例示して説明する。なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054の登録は既に終了しているものとする。

【0402】ステップS21: EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKcp,pの公開鍵証明書CERcpを、自らの署名データSIG1,escと共にコンテンツプロバイダ301に送信する。また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKsp,pの公開鍵証明書CERspを、自らの署名データSIG1,escと共にサービスプロバイダ310に送信する。また、EMDサービスセンタ302は、各々有効期限が1カ月の3カ月のライセンス鍵データKD1～KD3をユーザホームネットワーク303のSAM3051～3054に送信する。

【0403】ステップS22: コンテンツプロバイダ301は、相互認証を行った後に、権利書データ106およびコンテンツ鍵データKcをEMDサービスセンタ302に登録して権威化する。また、EMDサービスセンタ302は、図3(B)に示す6カ月のキーファイルKFを作成し、これをコンテンツプロバイダ301に送信する。

【0404】ステップS23: コンテンツプロバイダ3

121

01は、図3(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG6.SPと、キーファイルKFおよびその署名データSIG7.SPを作成し、これらと図3(C)に示す公開鍵証明書データCERapおよびその署名データSIG1.Escとを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、サービスプロバイダ310に提供する。

【0405】ステップS24：サービスプロバイダ310は、図3(C)に示す署名データSIG1.Escを検証した後に、公開鍵証明書データCERapに格納された公開鍵データKcp.Pを用いて、図3(A)、(B)に示す署名データSIG6.SPおよびSIG7.SPを検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0406】ステップS25：サービスプロバイダ310は、プライスタグデータ312およびその署名データSIG64.SPを作成し、これらを格納した図65に示すセキュアコンテナ304を作成する。

【0407】ステップS26：サービスプロバイダ310は、プライスタグデータ312をEMDサービスセンタ302に登録して権威化する。

【0408】ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図74に示すネットワーク機器3601の復号モジュール905に送信する。

【0409】ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0410】ステップS29：SAM3051～3054のいずれかにおいて、図87(D)に示す署名データSIG61.Escを検証した後に、公開鍵証明書データCERspに格納された公開鍵データKsp.Pを用いて、図87(A)、(B)、(C)に示す署名データSIG62.SP、SIG63.SP、SIG64.SPを検証して、セキュアコンテナ304内の所定のデータが正当なサービスプロバイダ310において作成および送信されたか否かを確認する。

【0411】ステップS30：SAM3051～3054のいずれかにおいて、図87(D)に示す署名データSIG1.Escを検証した後に、公開鍵証明書データCERcpに格納された公開鍵データKcp.Pを用いて、図87(A)、(B)、(C)に示す署名データSIG6.SP、SIG7.SPを検証して、セキュアコンテナ304内のコンテンツファイルCFが正当なコンテンツプロバイダ301において作成されたか否かと、キーファイルKFが正当なコンテンツプロバイダ301から送信されたか否かを確認する。また、SAM3051～3054のい

122

れかにおいて、公開鍵データKEsc.Pを用いて、図87(B)に示すキーファイルKF内の署名データSIGK1.Escの正当性を検証することで、キーファイルKFが正当なEMDサービスセンタ302によって作成されたか否かを確認する。

【0412】ステップS31：ユーザが図91の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

【0413】ステップS32：ステップS31において生成された操作信号S165に基づいて、SAM3051～3054において、セキュアコンテナ304の利用履歴(Usage Log)データ308が生成される。SAM3051～3054からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG205.SAM1が送信される。また、購入形態が決定される度にリアルタイムに、SAM3051～3054からEMDサービスセンタ302に利用制御状態データ166が送信される。

【0414】ステップS33：EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152c、152sを作成する。

【0415】ステップS34：EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0416】以上説明したように、EMDシステム300では、図3に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM3051～3054内で行う。また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD1～KD3を用いて暗号化されており、配信鍵データKD1～KD3を保持しているSAM3051～3054内でのみ復号される。そして、SAM3051～3054では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

【0417】従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデ

ータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ301の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300によれば、権利書データ106をサービスプロバイダ310が管理できないようである。そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303のSAMにおける当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0418】また、EMDシステム300では、セキュアコンテナ104、304内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ310およびSAM3051～3054において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータCの不正利用を効果的に回避できる。

【0419】また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク303へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM3051～3054におけるコンテンツデータCの権利処理を共通化できる。

【0420】また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器3601およびAV機器3602～3604においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。例えば、図107に示すように、コンテンツプロバイダ301が提供したコンテンツデータCを、サービスプロバイダ310からユーザホームネットワーク303に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク303、303aのSAMにおいて、コンテンツプロバイダ301が作成した権利書データ106に基づいて、共通の権利処理ルールが採用される。

【0421】また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。また、EMDシステム300によれば、同

じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM3051～3054に供給される。従って、SAM3051～3054において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0422】以下、上述した第2実施形態のEMDシステム300で採用するセキュアコンテナなどの配送プロトコルについて説明する。図108に示すように、コンテンツプロバイダ301において作成されたセキュアコンテナ104は、インターネット（TCP/IP）あるいは専用線（ATM Cell）などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ310に提供される。また、サービスプロバイダ310は、セキュアコンテナ104を用いて作成したセキュアコンテナ304を、デジタル放送（MPEG-TS上のXML/SMIL）、インターネット（TCP/IP上のXML/SMIL）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク303に配給する。また、ユーザホームネットワーク303、303a内、あるいはユーザホームネットワーク303と303aとの間において、SMA相互間で、セキュアコンテナが、家庭内EC(Electric Commerce)/配信サービス（1394シリアルバス・インターフェイス上のXML/SMIL）や記録媒体などを用いて転送される。

【0423】本発明は上述した実施形態には限定されない。例えば、上述した実施形態では、EMDサービスセンタ102、302において、キーファイルKFを作成する場合を例示したが、コンテンツプロバイダ101、301においてキーファイルKFを作成してもよい。

【0424】

【発明の効果】以上説明したように、本発明のデータ処理装置によれば、コンテンツデータの取り扱いを示す権利書データに基づいてコンテンツデータの購入形態等を決定できる。その結果、権利書データをコンテンツデータの提供に係わる者が作成すれば、コンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図1】図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】図2は、本発明のセキュアコンテナの概念を説

明するための図である。

【図3】図3は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテンツのフォーマットを説明するための図である。

【図4】図4は、図3に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図5】図5は、図3に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図6】図6は、図1に示すコンテンツプロバイダとEMDサービスセンタとの間で行われる登録およびキーファイルの転送を説明するための図である。

【図7】図7は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図8】図8は、コンテンツIDを説明するための図である。

【図9】図9は、セキュアコンテンツのディレクトリ構造を説明するための図である。

【図10】図10は、セキュアコンテンツのハイパーリンク構造を説明するための図である。

【図11】図11は、本実施形態で用いられるROM型の記録媒体の第1の例を説明するための図である。

【図12】図12は、本実施形態で用いられるROM型の記録媒体の第2の例を説明するための図である。

【図13】図13は、本実施形態で用いられるROM型の記録媒体の第3の例を説明するための図である。

【図14】図14は、本実施形態で用いられるRAM型の記録媒体の第1の例を説明するための図である。

【図15】図15は、本実施形態で用いられるRAM型の記録媒体の第2の例を説明するための図である。

【図16】図16は、本実施形態で用いられるRAM型の記録媒体の第3の例を説明するための図である。

【図17】図17は、コンテンツプロバイダにおけるセキュアコンテンツの作成処理の手順を示すフローチャートである。

【図18】図18は、コンテンツプロバイダにおけるセキュアコンテンツの作成処理の手順を示すフローチャートである。

【図19】図19は、コンテンツプロバイダにおけるセキュアコンテンツの作成処理の手順を示すフローチャートである。

【図20】図20は、図1に示すEMDサービスセンタの機能を示す図である。

【図21】図21は、図1に示す利用履歴データを説明するための図である。

【図22】図22は、図1に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図23】図23は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図である。

【図24】図24は、図22に示す外部メモリに記憶されるデータを説明するための図である。

【図25】図25は、作業用メモリに記憶されるデータを説明するための図である。

【図26】図26は、図1に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図27】図27は、図23に示す記憶部に記憶されるデータを説明するための図である。

【図28】図28は、EMDサービスセンタからライセンス鍵データを受信する際のSAMの処理を示すフローチャートである。

【図29】図29は、セキュアコンテンツを入力する際のSAMの処理を示すフローチャートである。

【図30】図30は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図31】図31は、コンテンツデータの購入形態を決定する際のSAMの処理を示すフローチャートである。

【図32】図32は、購入形態が決定されたセキュアコンテンツを説明するための図である。

【図33】図33は、コンテンツデータを再生する際のSAMの処理を示すフローチャートである。

【図34】図34は、図22に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送し、AV機器において再購入を行う場合を説明するための図である。

【図35】図35は、図34に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図36】図36は、図34に示す処理を示すフローチャートである。

【図37】図37は、図34において転送されるセキュアコンテンツのフォーマットを説明するための図である。

【図38】図38は、図34に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図39】図39は、図34に示す場合における転送先のSAMの処理を示すフローチャートである。

【図40】図40は、図34に示す場合における転送先のSAMの処理を示すフローチャートである。

【図41】図41は、図1に示すユーザホームネットワーク内のSAMにおける各種の購入形態を説明するための図である。

【図42】図42は、コンテンツの購入形態が未決定の図11に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する場合を説明するための図である。

【図 43】図 43 は、図 42 に示す場合における AV 機器の SAM 内でのデータの流れを示す図である。

【図 44】図 44 は、図 42 に示す場合における SAM の処理のフローチャートである。

【図 45】図 45 は、ユーザホームネットワーク内の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテンツを読み出して、これを他の AV 機器に転送して RAM 型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 46】図 46 は、図 45 に示す場合における転送元の SAM 内でのデータの流れを示す図である。

【図 47】図 47 は、図 45 において、転送元の SAM から転送先の SAM に転送されるセキュアコンテンツのフォーマットを説明するための図である。

【図 48】図 48 は、図 45 の場合における、転送元および転送先の SAM の処理のフローチャートを示す図である。

【図 49】図 49 は、図 45 の場合における、転送元および転送先の SAM の処理のフローチャートを示す図である。

【図 50】図 50 は、図 45 に示す場合における転送先の SAM 内でのデータの流れを示す図である。

【図 51】図 51 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 52】図 52 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 53】図 53 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図 54】図 54 は、SAM が作成する SAM 登録リストのデータフォーマットを説明するための図である。

【図 55】図 55 は、EMD サービスセンタが作成する公開鍵証明書破棄リストのフォーマットを説明するための図である。

【図 56】図 56 は、EMD サービスセンタが作成する SAM 登録リストのデータフォーマットを説明するための図である。

【図 57】図 57 は、SAM が持つセキュリティ機能を説明するための図である。

【図 58】図 58 は、コンテンツプロバイダからネットワーク機器に送信されたセキュアコンテンツに格納されたコンテンツデータを AV 機器（ストレージ機器）において記録媒体（メディア）に書き込む際に行われる、コンテンツプロバイダ、SAM 相互間のセキュリティ機能を

説明するための図である。

【図 59】図 59 (A) は一般的に用いられる OSI 参照モデルにおける送信側および受信側の各層（レイヤー）で行われる通信を説明するための図、図 59 (B) は図 58 に示すコンテンツプロバイダとネットワーク機器（SAM）との間での通信時の保護機能を詳細に説明するための図である。

【図 60】図 60 は、図 58 に示すネットワーク機器（SAM）と AV 機器（SAM）との間の通信時の保護機能を詳細に説明するための図である。

【図 61】図 61 は、例えば、図 1 に示す一の AV 機器において図 11 に示す ROM 型の記録媒体からコンテンツデータを再生し、当該再生したコンテンツデータをバスを介して他の AV 機器に伝送し、当該他の AV 機器において図 14 に示す RAM 型の記録媒体に記録する場合のセキュリティ処理を説明するための図である。

【図 62】図 62 は、図 1 に示すユーザホームネットワーク内の例えばネットワーク機器内での各種の SAM に搭載形態の一例を説明するための図である。

【図 63】図 63 は、権利処理用の SAM の回路モジュールの第 1 形態を説明するための図である。

【図 64】図 64 は、図 63 に示す回路モジュールを用いた場合の SAM 内のハードウェア構成の一例を説明するための図である。

【図 65】図 65 は、権利処理用の SAM の回路モジュールの第 2 形態を説明するための図である。

【図 66】図 66 は、メディア SAM の回路モジュールの第 1 形態を説明するための図である。

【図 67】図 67 は、ROM 型の記録媒体のメディア SAM の出荷時における記憶データを説明するための図である。

【図 68】図 68 は、ROM 型の記録媒体のメディア SAM の登録後における記憶データを説明するための図である。

【図 69】図 69 は、RAM 型の記録媒体のメディア SAM の出荷時における記憶データを説明するための図である。

【図 70】図 70 は、RAM 型の記録媒体のメディア SAM の登録後における記憶データを説明するための図である。

【図 71】図 71 は、メディア SAM の回路モジュールの第 2 形態を説明するための図である。

【図 72】図 72 は、メディア SAM の回路モジュールの第 3 形態を説明するための図である。

【図 73】図 73 は、メディア SAM の回路モジュールの第 4 形態を説明するための図である。

【図 74】図 74 は、メディア SAM の回路モジュールの第 5 形態を説明するための図である。

【図 75】図 75 は、メディア SAM の回路モジュールの第 6 形態を説明するための図である。

【図76】図76は、メディアSAMの回路モジュールの第7形態を説明するための図である。

【図77】図77は、AV圧縮・伸長用SAMの回路モジュールの第1形態を説明するための図である。

【図78】図78は、AV圧縮・伸長用SAMの回路モジュールの第2形態を説明するための図である。

【図79】図79は、メディア・ドライブSAMの回路モジュールの第1形態を説明するための図である。

【図80】図80は、メディア・ドライブSAMの回路モジュールの第2形態を説明するための図である。

【図81】図81は、メディア・ドライブSAMの回路モジュールの第3形態を説明するための図である。

【図82】図82は、メディア・ドライブSAMの回路モジュールの第4形態を説明するための図である。

【図83】図83は、図1に示すEMDシステムの全体動作のフローチャートである。

【図84】図84は、第1実施形態のEMDシステムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図85】図85は、本発明の第2実施形態のEMDシステムの全体構成図である。

【図86】図86は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図87】図87は、図85に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図88】図88は、図87に示すセキュアコンテナに格納されたコンテンツファイルの送信形態を説明するための図である。

【図89】図89は、図87に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図90】図90は、図85に示すEMDサービスセンタの機能を示す図である。

【図91】図91は、図85に示すネットワーク機器の構成図である。

【図92】図92は、図91に示すCAモジュールの機能ブロック図である。

【図93】図93は、図85に示すSAMの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図94】図94は、図93に示す作業用メモリに記憶されるデータを説明するための図である。

【図95】図95は、図85に示すSAMの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図96】図96は、図85に示すSAMにおけるセキュアコンテナの入力処理の手順を示すフローチャートである。

【図97】図97は、図85に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合を説明するための図である。

【図98】図98は、図85に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAM内での処理の流れを説明するための図である。

【図99】図99は、図98に示す転送元のSAMの処理を示すフローチャートである。

【図100】図100は、図97に示す場合に、転送元のSAMから転送先のSAMに転送されるセキュアコンテナのフォーマットを示す図である。

【図101】図101は、図97に示す場合の転送先のSAM内でのデータの流れを示す図である。

【図102】図102は、図97に示す場合の転送先のSAMの処理のフローチャートである。

【図103】図103は、図97に示す場合の転送先のSAMの処理のフローチャートである。

【図104】図104は、図85に示すユーザホームネットワーク内でのSAMの接続形態の一例を説明するための図である。

【図105】図105は、図85に示すEMDシステムの全体動作のフローチャートである。

【図106】図106は、図85に示すEMDシステムの全体動作のフローチャートである。

【図107】図107は、図85に示すEMDシステムのサービス形態の一例を示す図である。

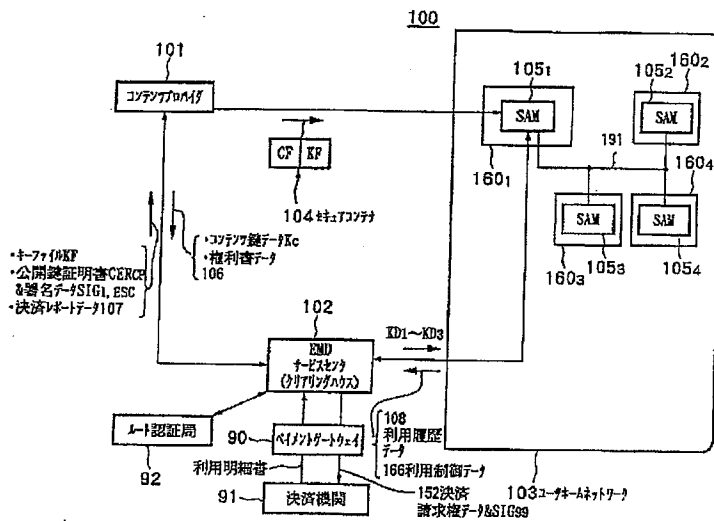
【図108】図108は、図85に示すEMDシステムにおいて採用されるセキュアコンテナの配送プロトコルを説明するための図である。

【図109】図109は、従来のEMDシステムの構成図である。

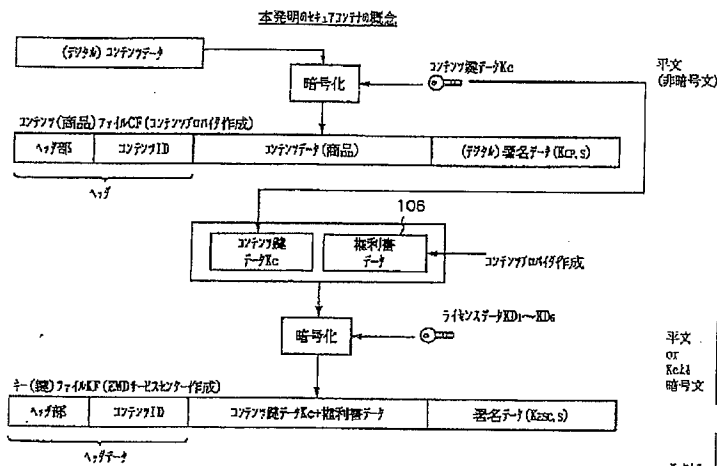
【符号の説明】

90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100、300…EMDシステム、101、301…コンテンツプロバイダ、102、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、105₁～105₄、305₁～305₄…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV機器、152、152_c、152_s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

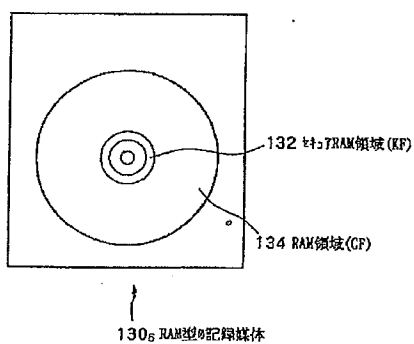
【図 1】



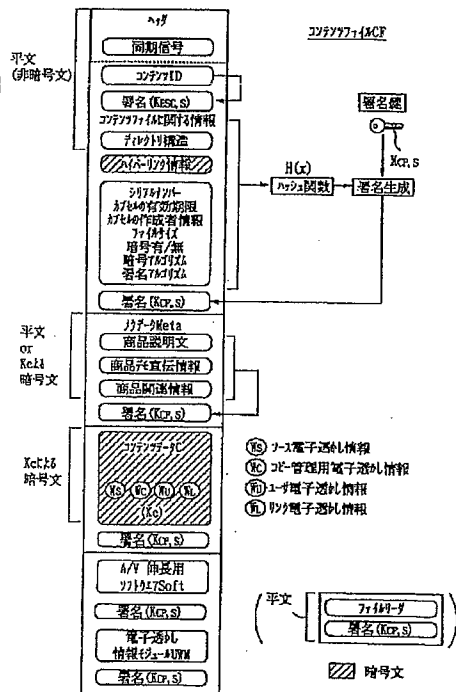
【図 2】



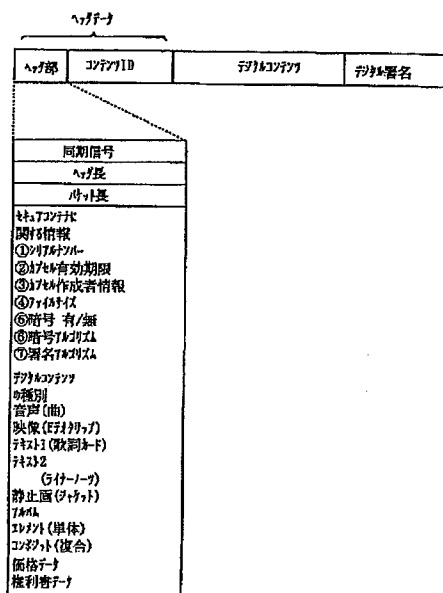
【図 16】



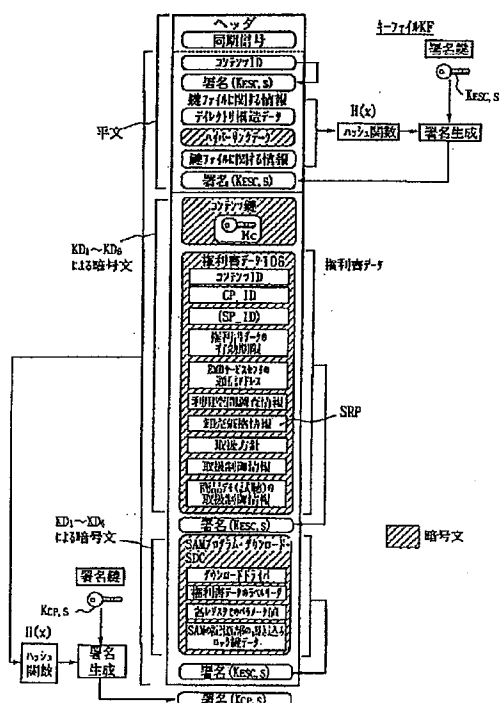
【図4】



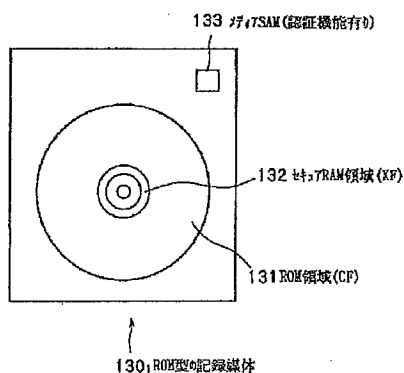
【図 7】



【図 5】



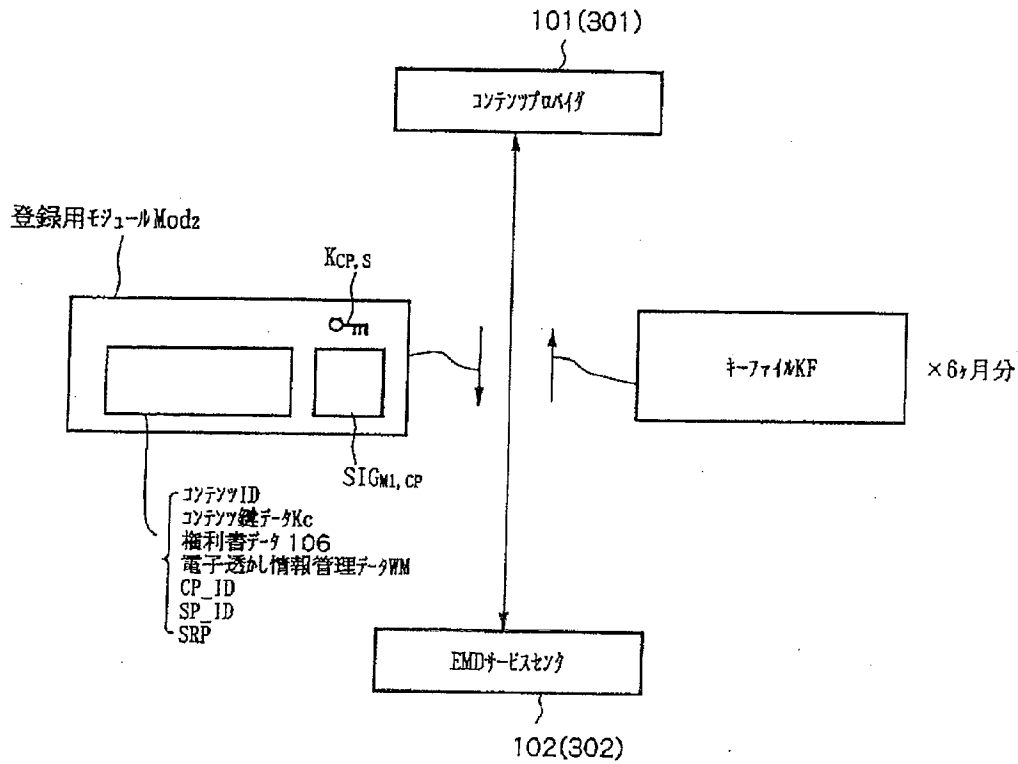
【图 1-1】



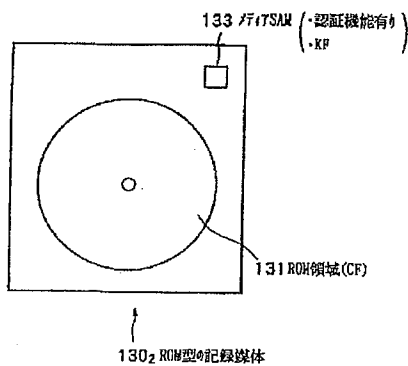
【图 24】

(KF:ダウノート・メモリにメモIF SAMが無い場合)

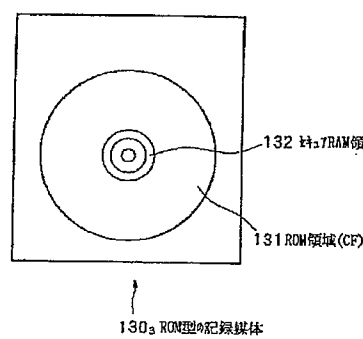
【図6】



【図12】



【図13】



【図25】

作業用メモリ200に記憶されるデータ

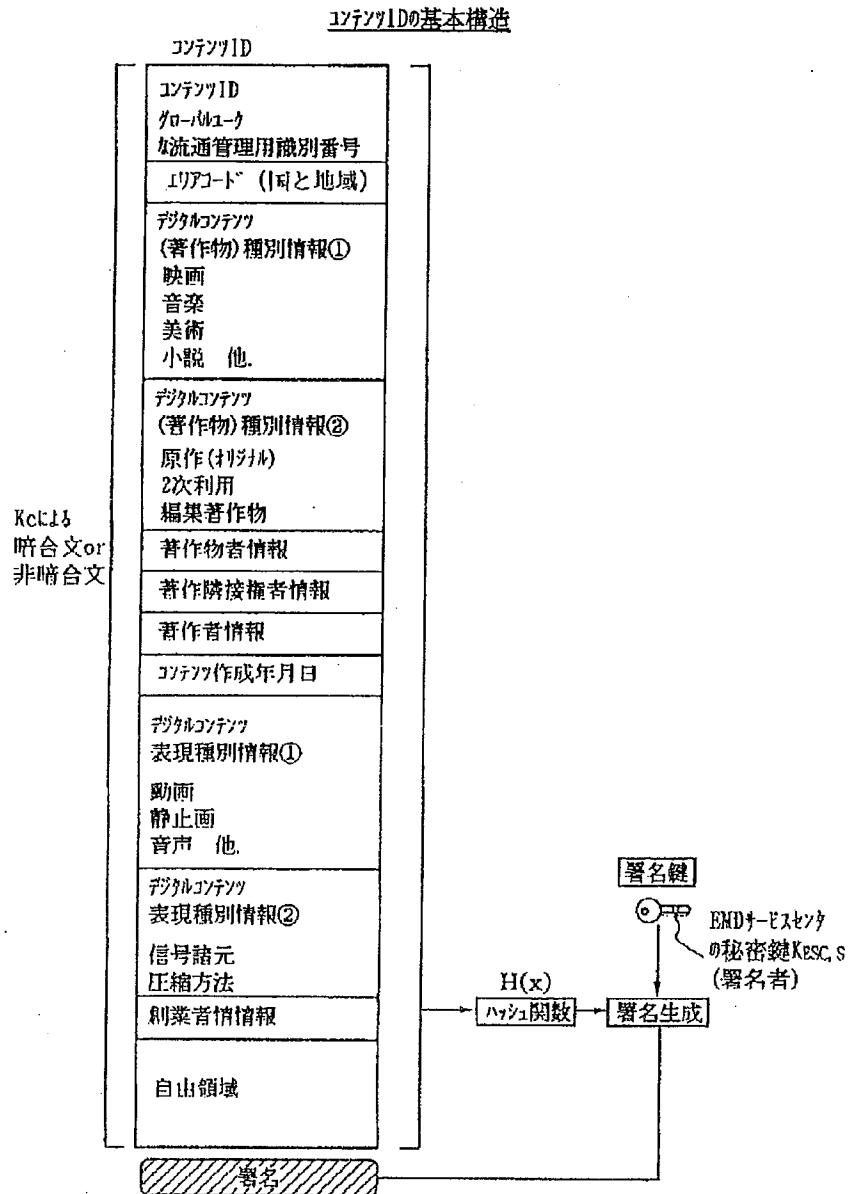
コンテンツ鍵データKc
権利者データ(UCP)106
記憶部(フラッシュメモリ)192000ビット鍵データKLoc
コンテンツプロバイダ101の公開鍵証明書CERCP
利用制御データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD1～SDC4

【図94】

作業用メモリ200に記憶されるデータ

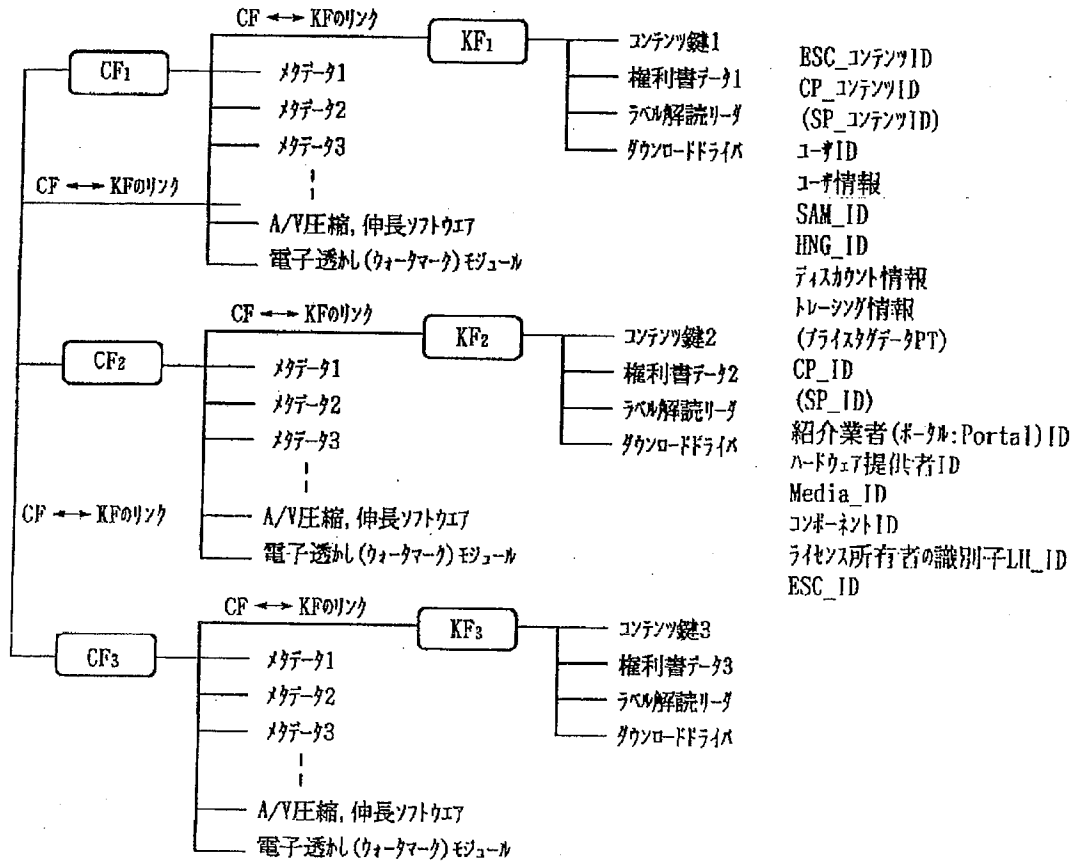
コンテンツ鍵データKc
権利者データ(UCP)106
不揮発性メモリ201000ビット鍵データKLoc
コンテンツプロバイダ301の公開鍵証明書CERCP
サービスプロバイダ301の公開鍵証明書CERSP
利用制御データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD1～SDC4
プレイステーション312

【図8】

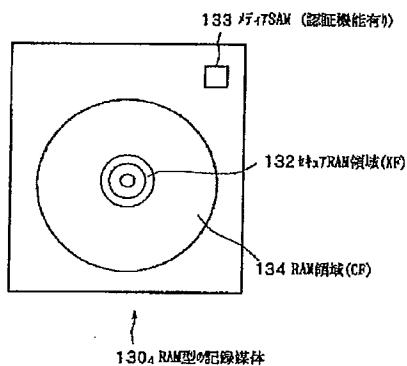


【図9】

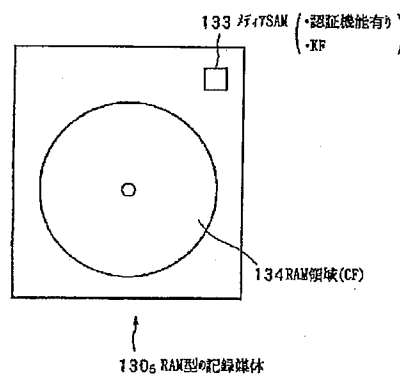
セキュリティコンテナのディレトリ構造



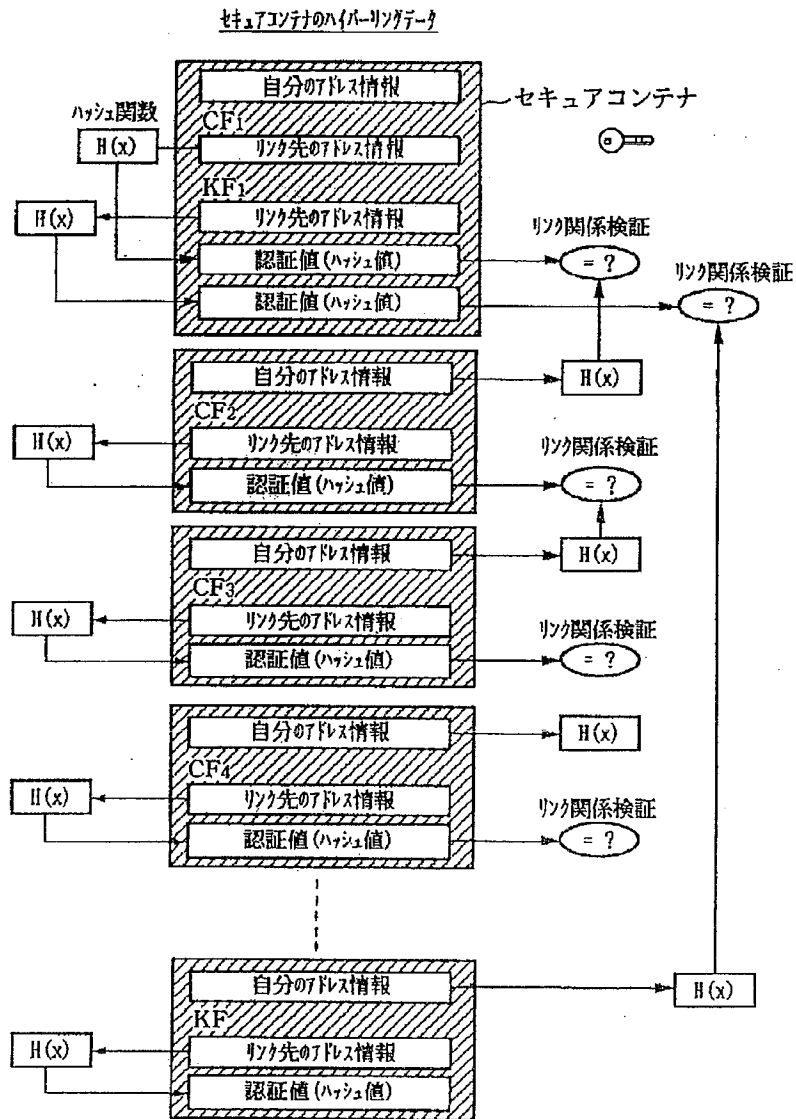
【図14】



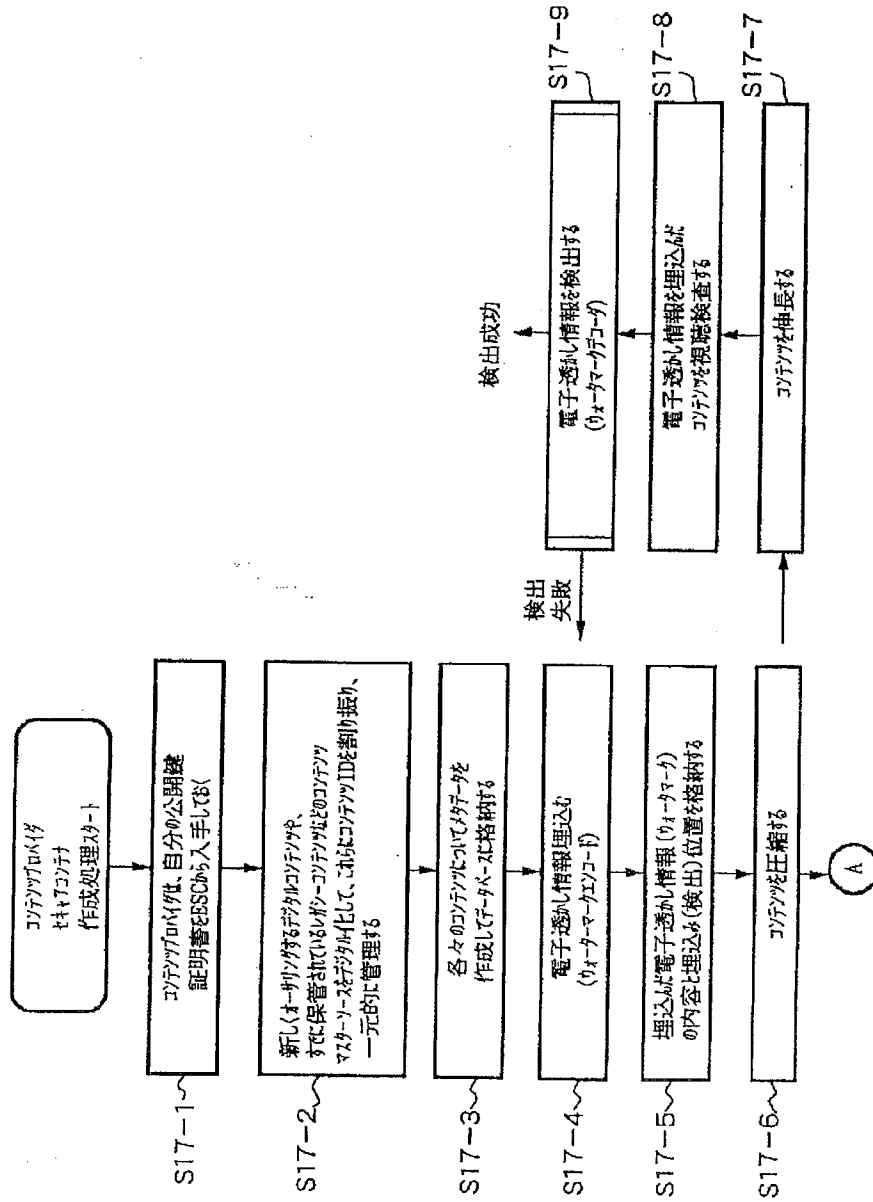
【図15】



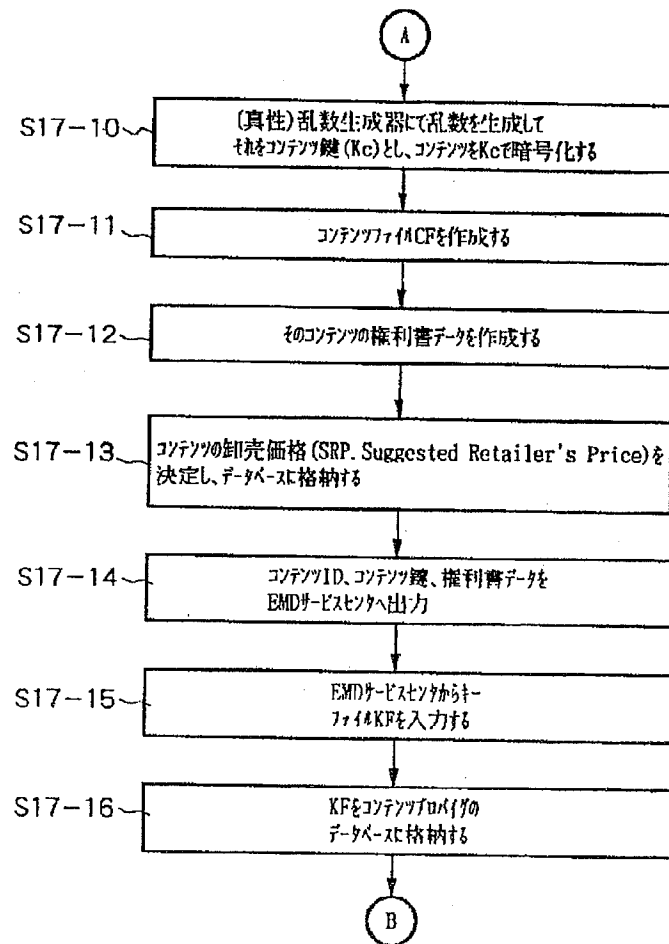
【図10】



【図17】



【図18】



ⓑ

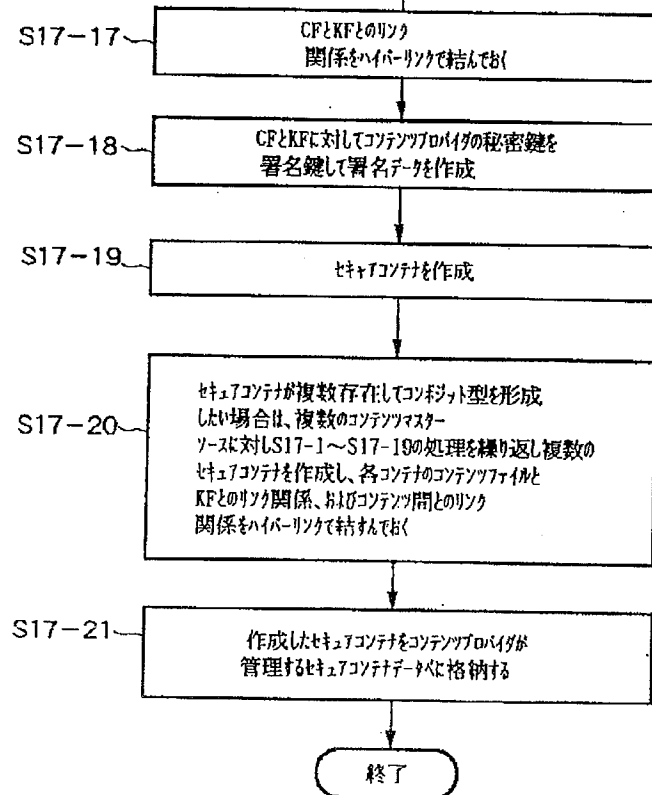
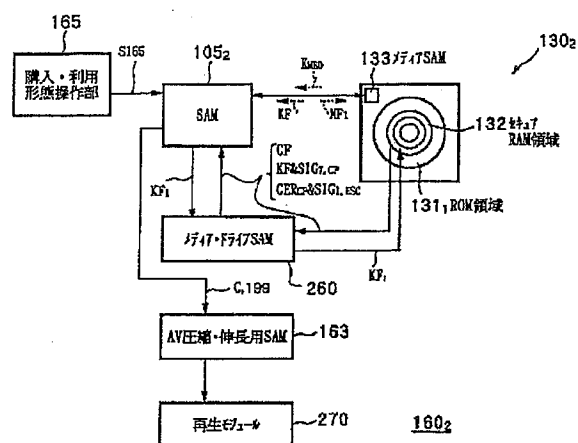


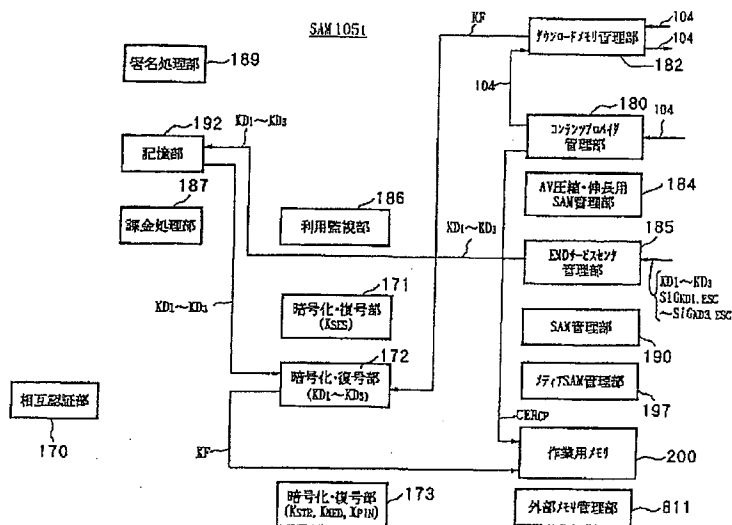
Figure 1 is a block diagram of a data recording system. The system is divided into two main sections: 160₁ (top) and 160₂ (bottom). Section 160₁ contains a '購入・利用形態操作部' (Purchase/Usage Form Operation Unit) 165, a 'SAM' (Security Access Module) 104, and a 'フロッピーディスク' (Floppy Disk) 167. Section 160₂ contains a '購入・利用形態操作部' 165, a 'SAM' 105₂, a 'ディスクドライブ' (Disk Drive) 133, and a 'ディスクドライブ SAM管理部' (Disk Drive SAM Management Unit) 260. Data flow is indicated by arrows: from 165 to 104, from 104 to 167, from 104 to 105₂, from 105₂ to 133, and from 133 to 260. Control lines are labeled with 'CF' and 'KF'. A label '104xデータ' is also present.

【圖 42】

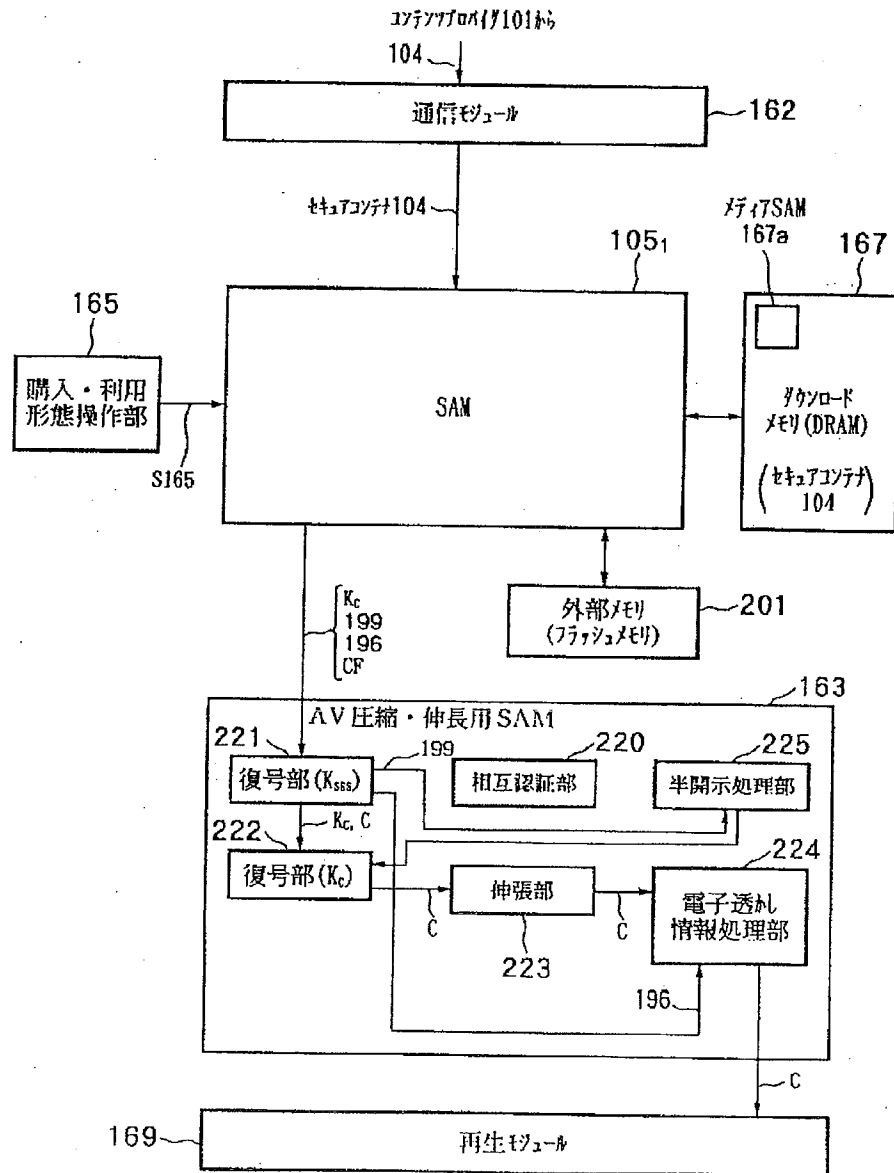
利用履歴データに基づく決済処理(利益分配処理)



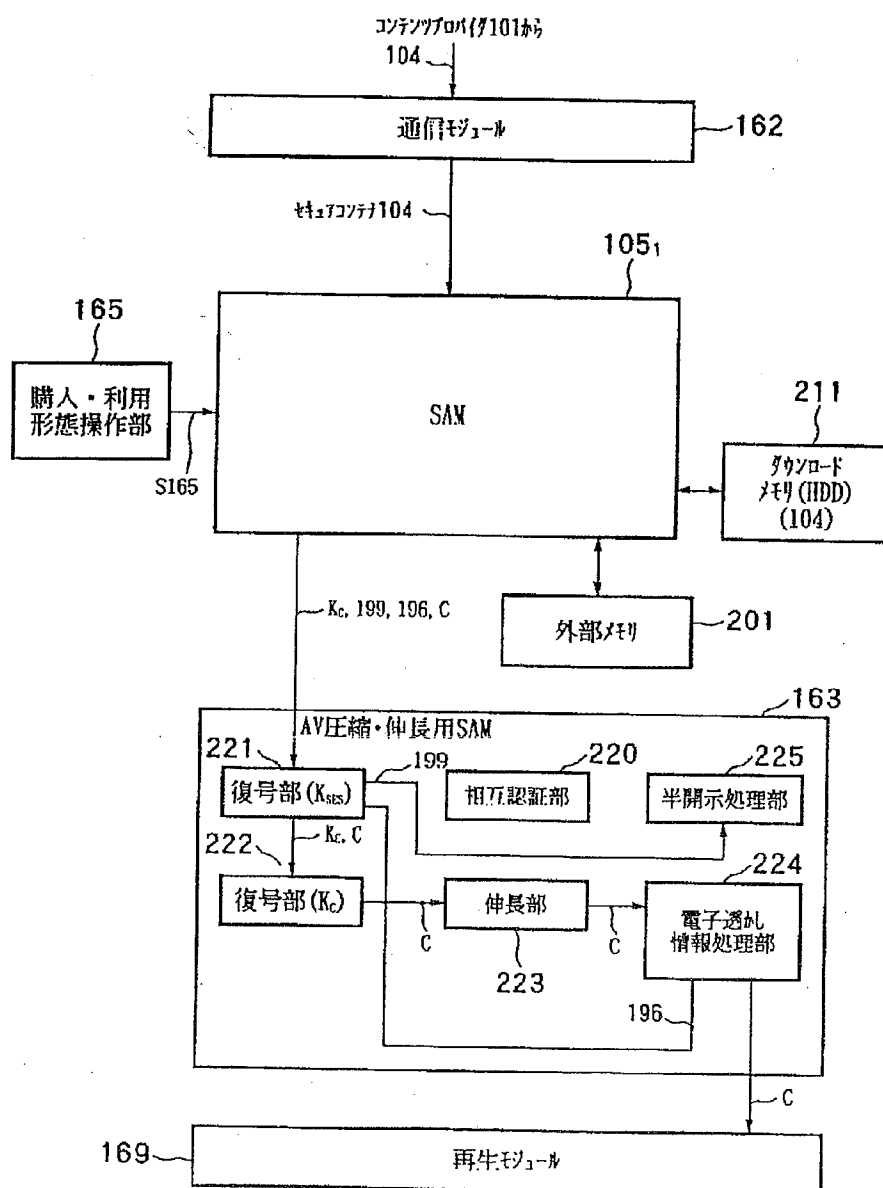
【図 23】



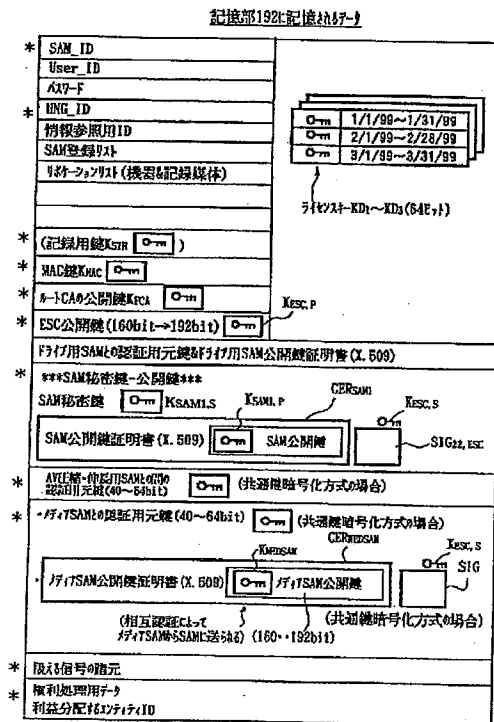
【図22】



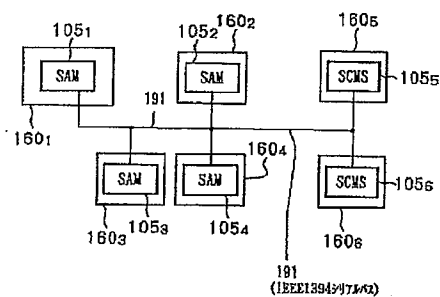
【図26】



【図27】

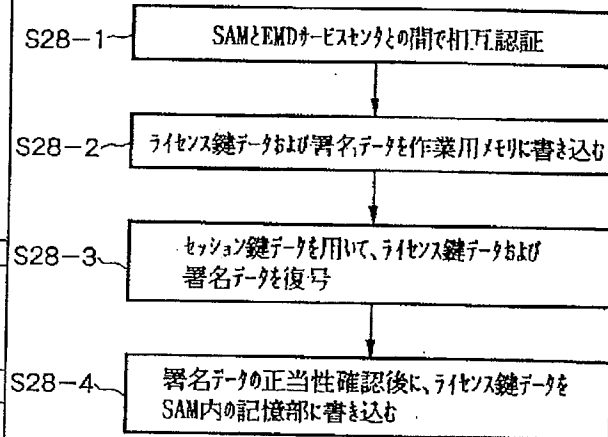


【図53】



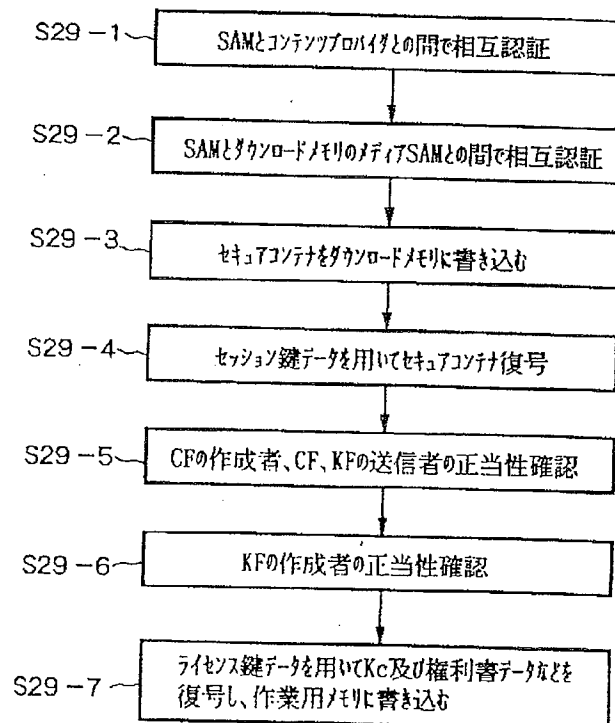
【図28】

ライセンス鍵データ受信処理 (SAM)



【図29】

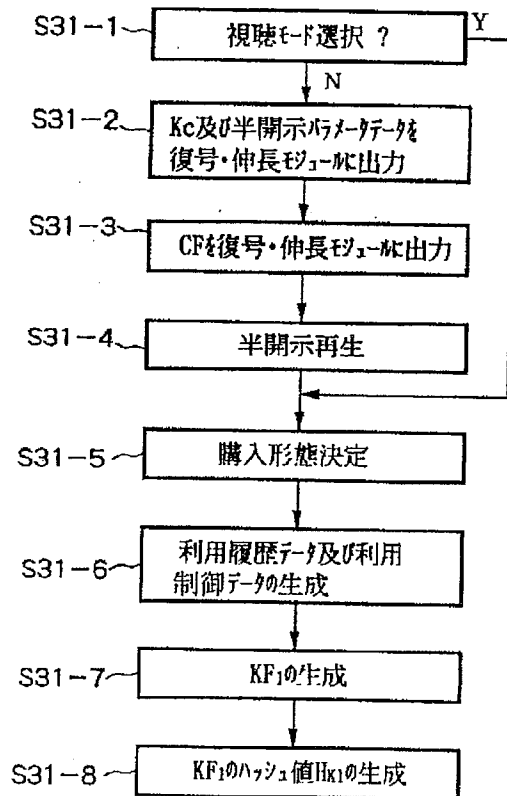
セキュアコンテナの入力処理 (SAM)



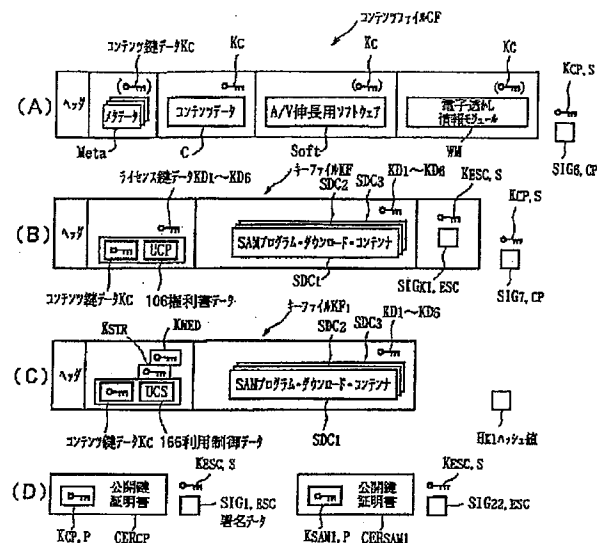
[illegible]

【図31】

購入形態決定処理

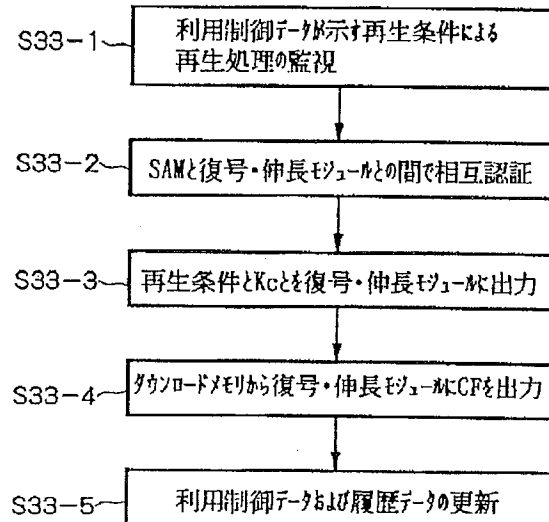


【図32】

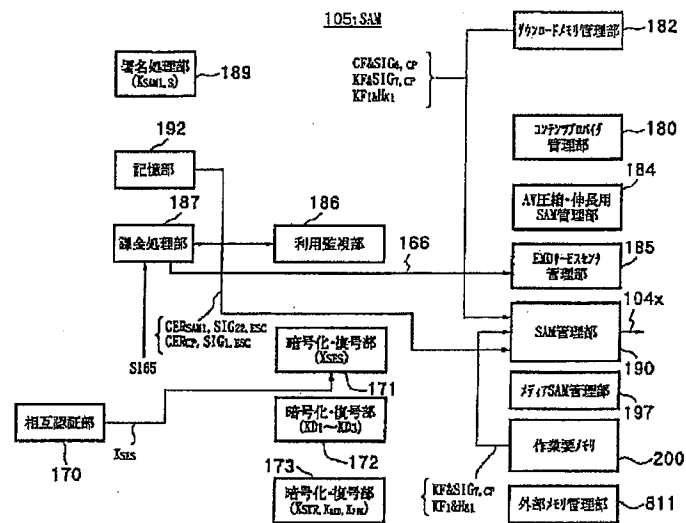


【図33】

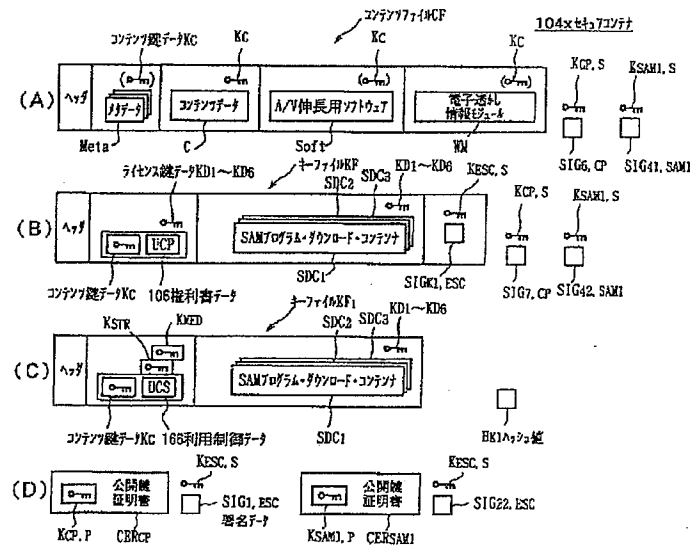
コンテンツデータの再生処理



【図35】

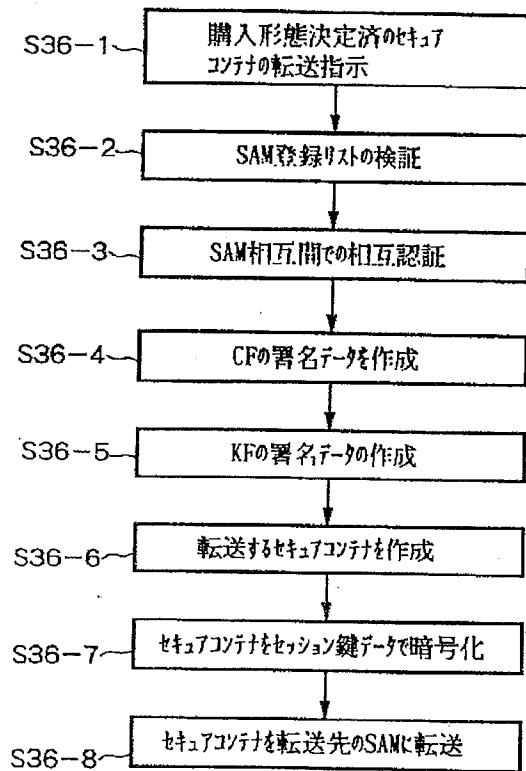


【図37】



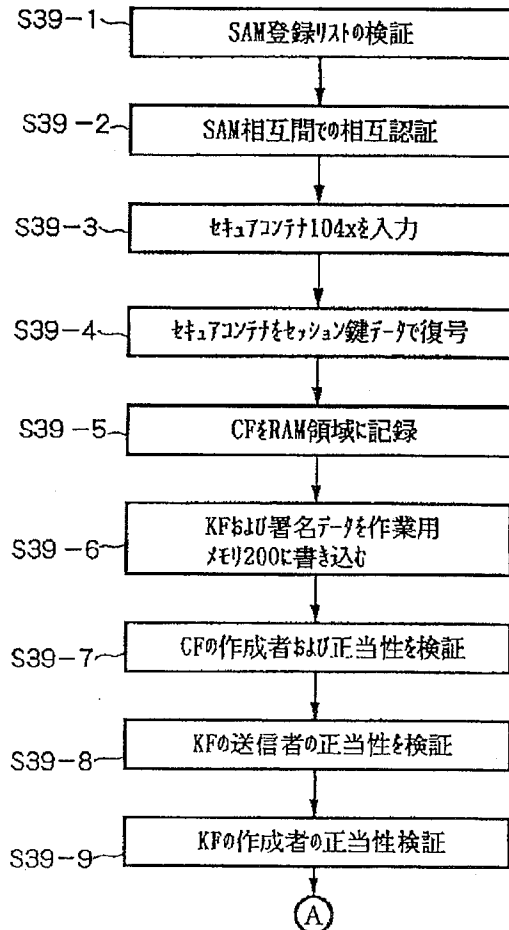
【図36】

一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理



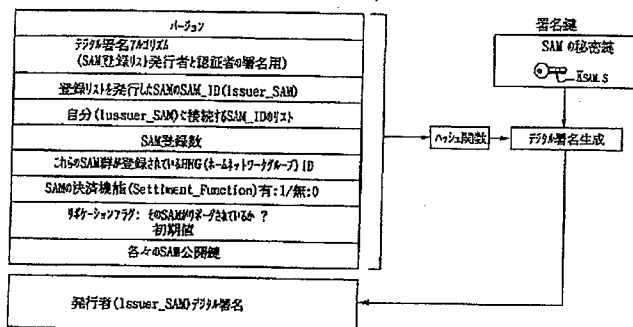
【図39】

一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理

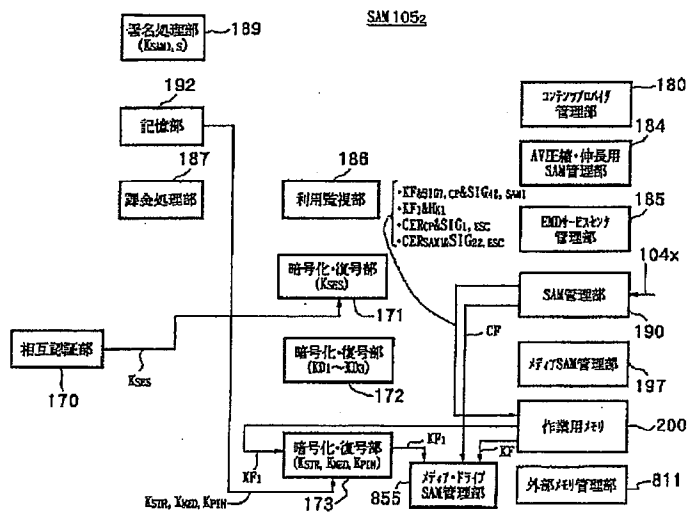


【図54】

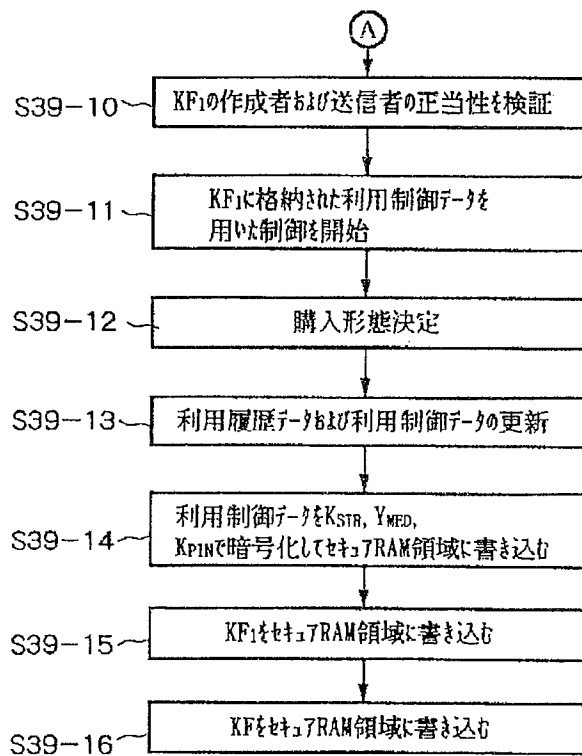
SAM登録リスト (SAM Registration List) (SAM作成)



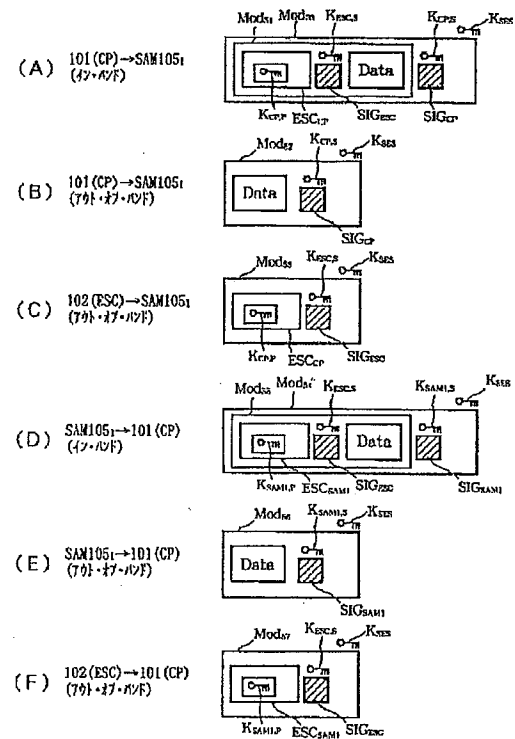
【図38】



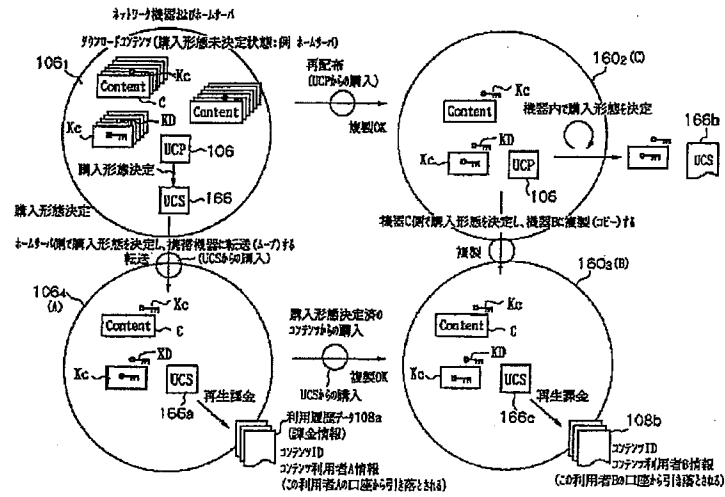
【図40】



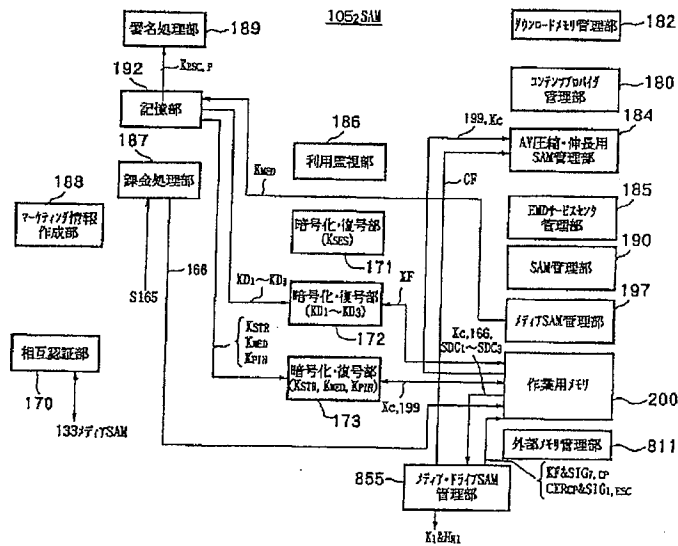
【図51】



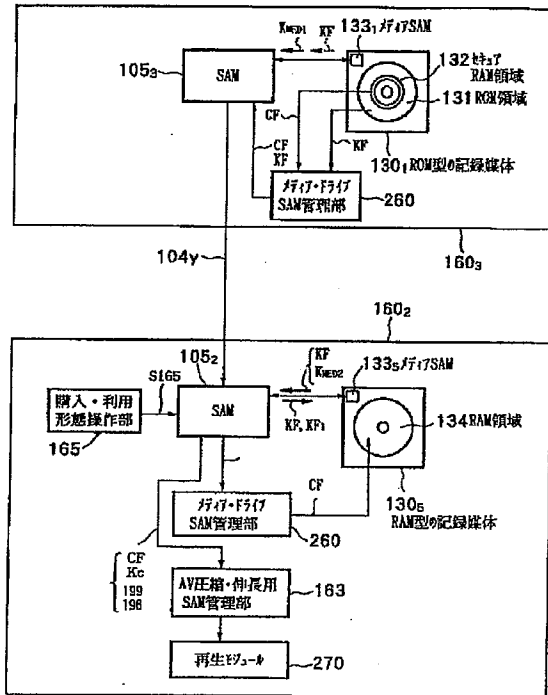
【図41】



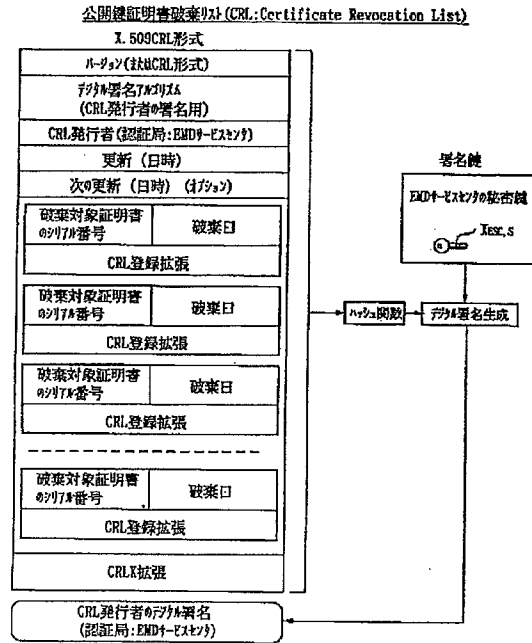
【図43】



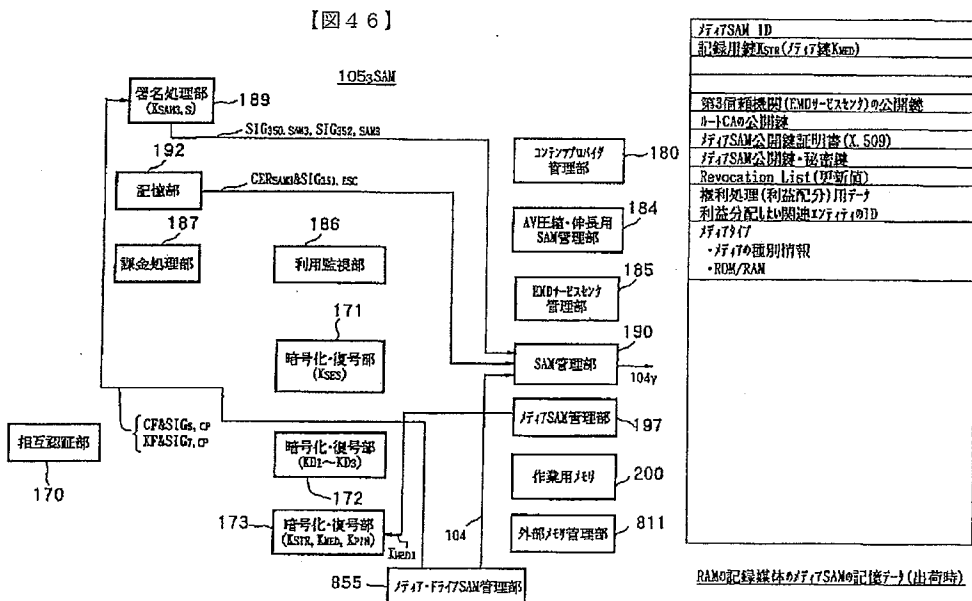
【図45】



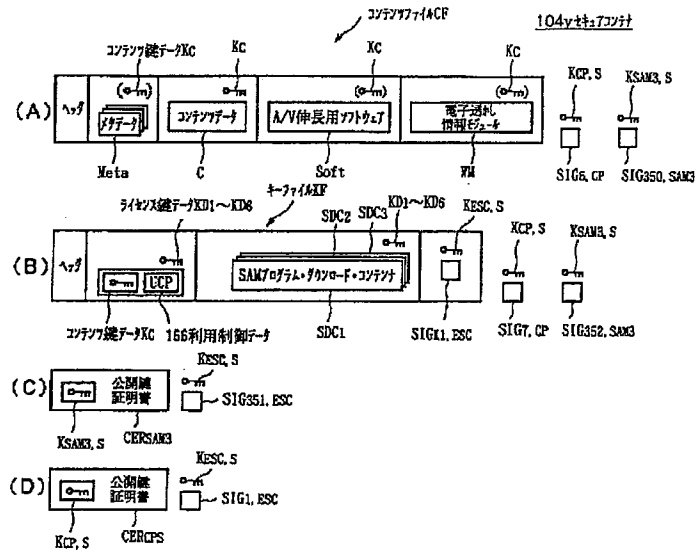
【図55】



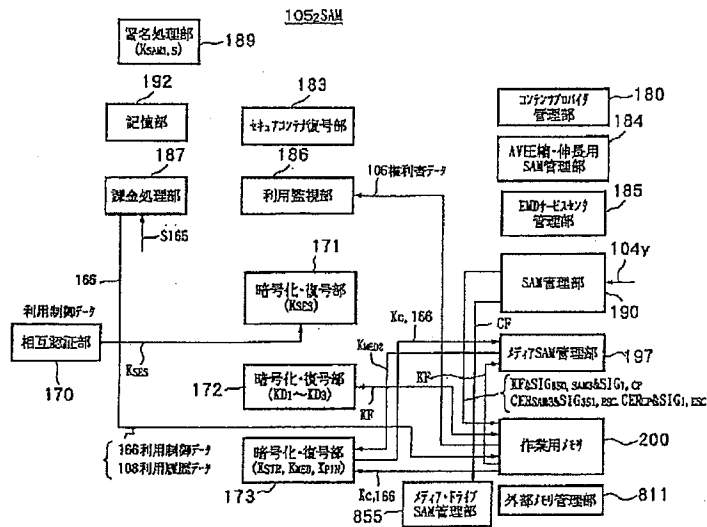
【図69】



【図47】

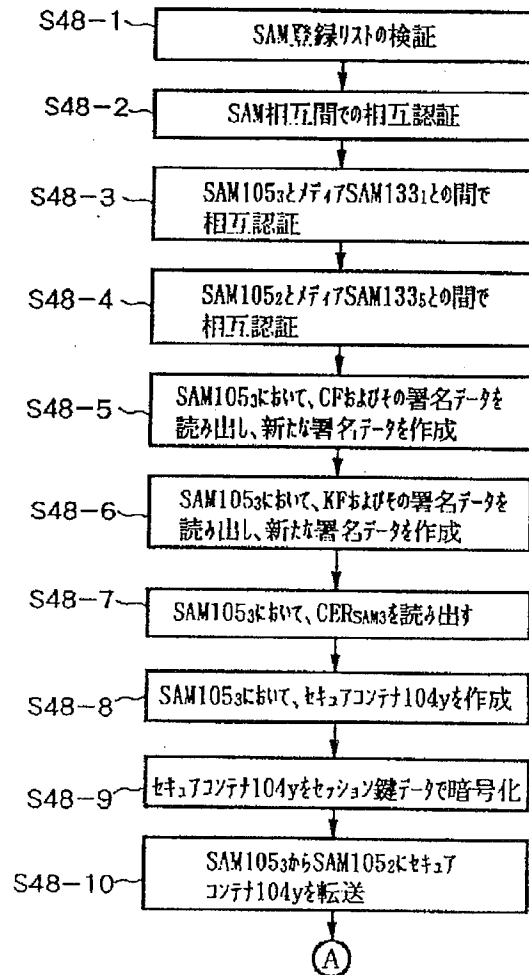


【図50】

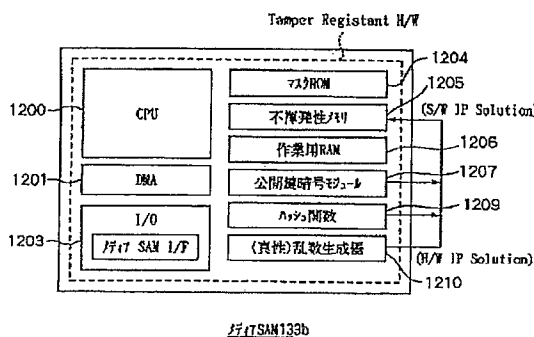


【図48】

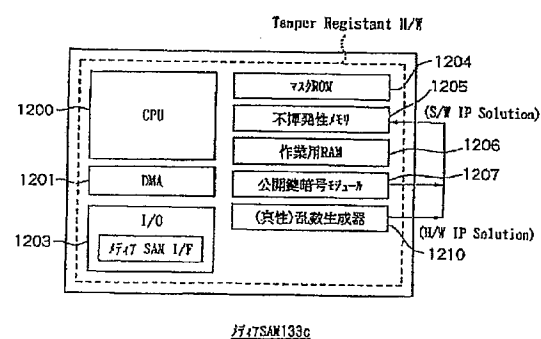
ROM型の記録媒体のコンテンツデータを転送した後転送先で
購入形態を決定してRAM型の記録媒体に書き込む場合の処理



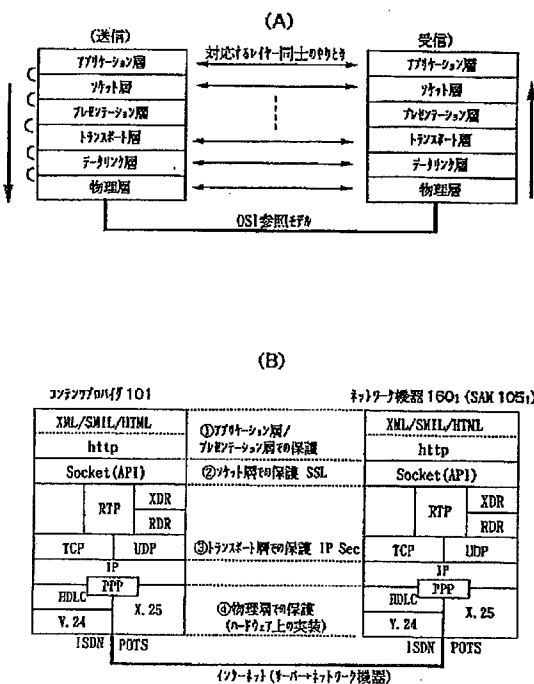
【図71】



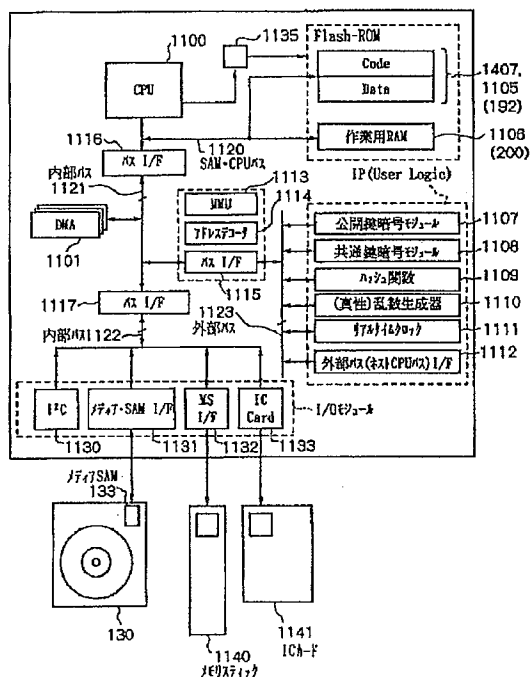
【図72】



【图 5 9】

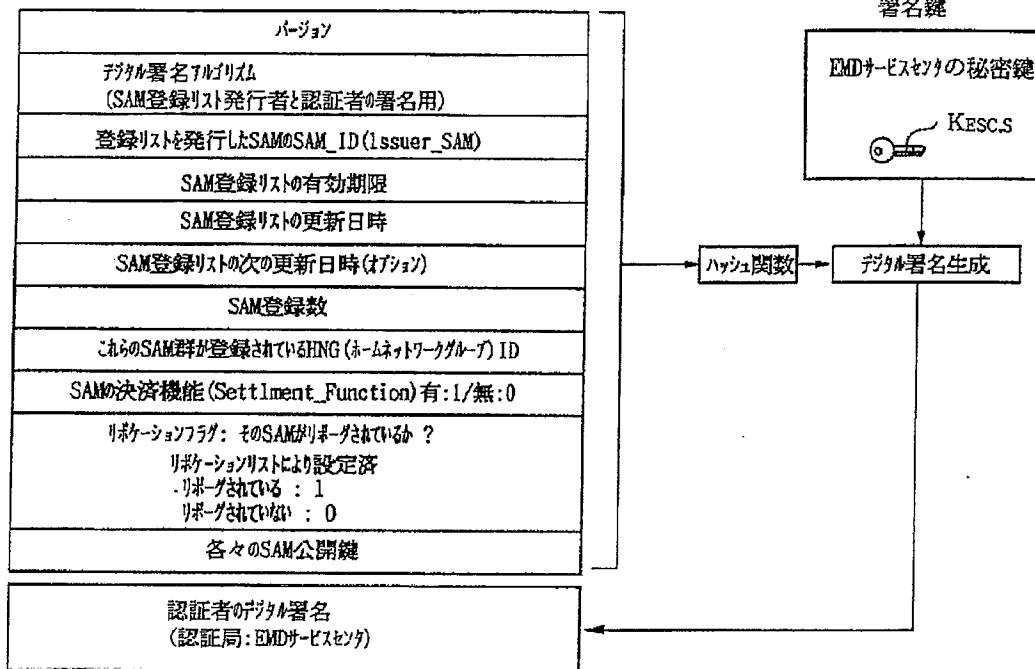


【図 6 4】

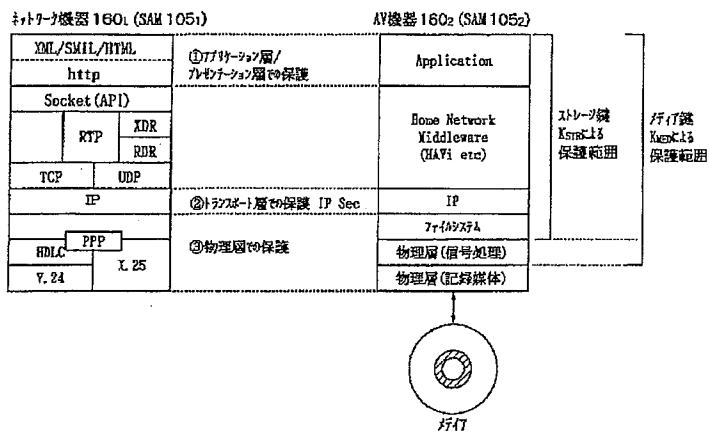


【図56】

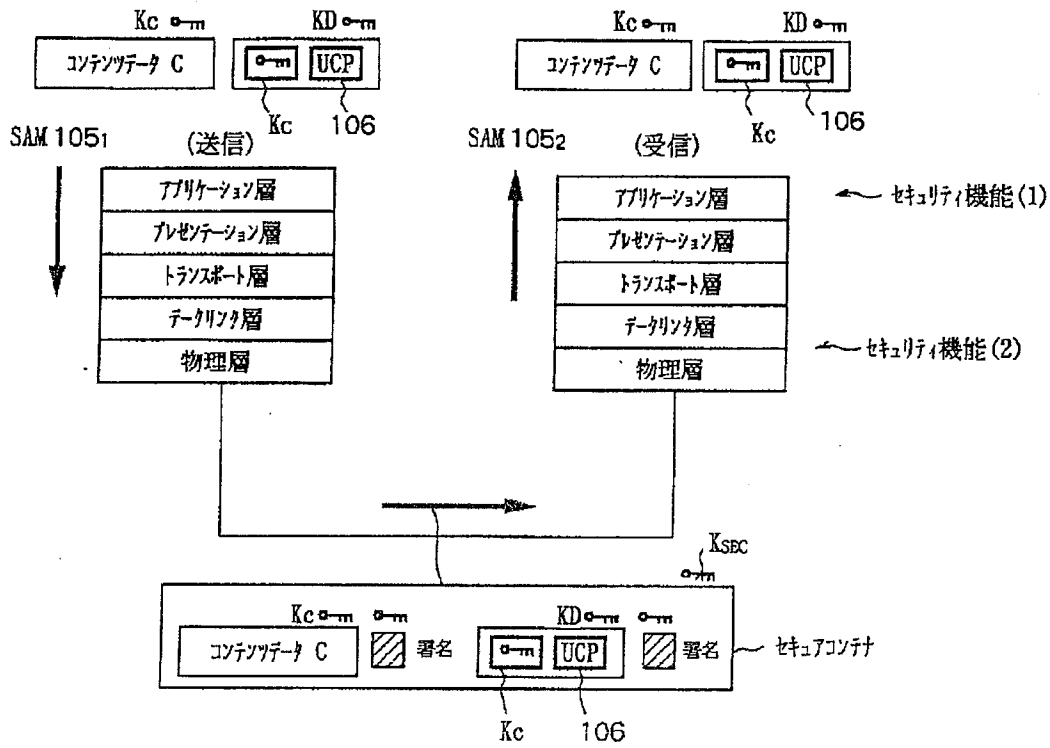
SAM登録リスト(EMDサービスセンサ作成)



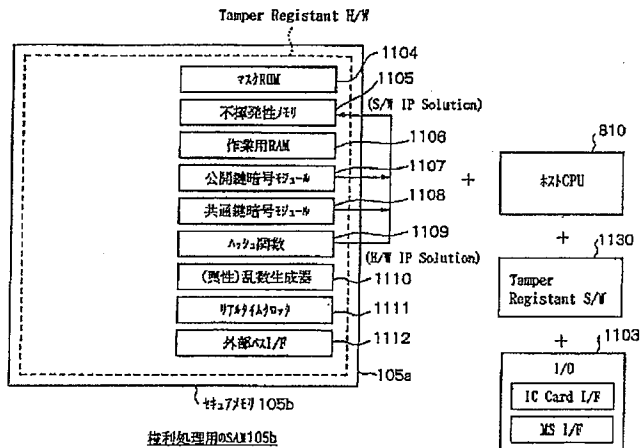
【図60】



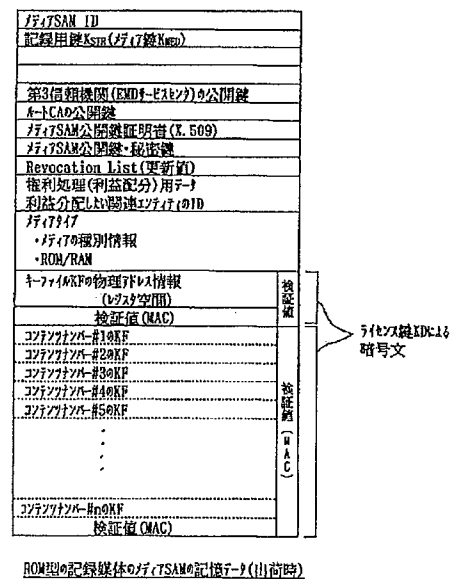
【図57】



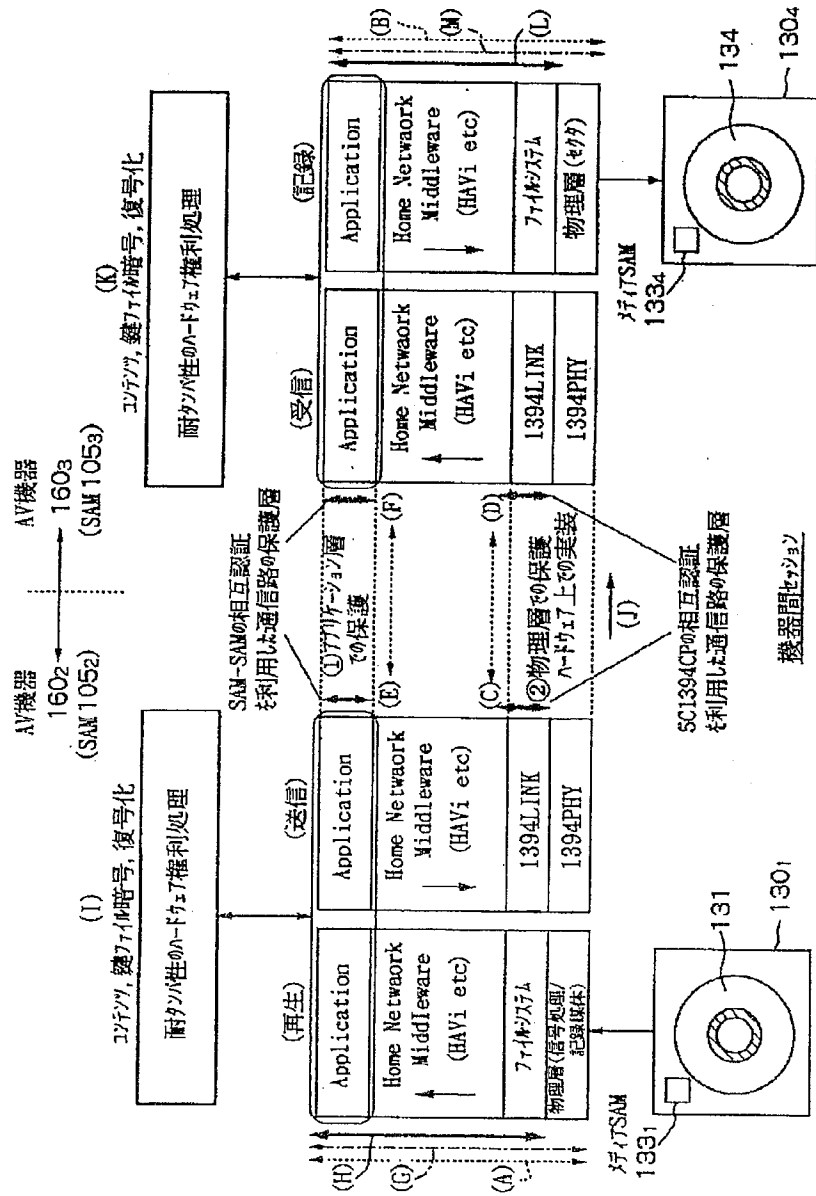
【図65】



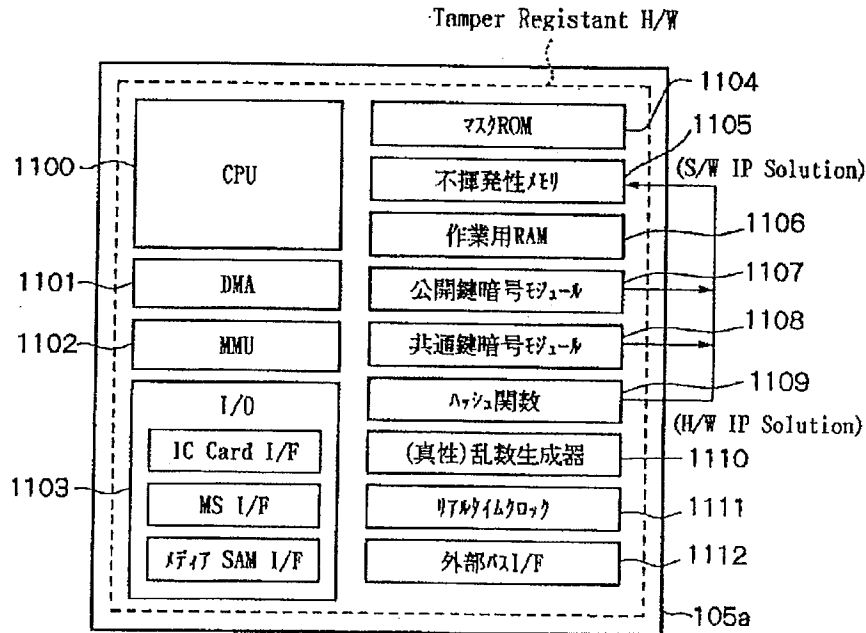
【図67】



【図61】



【図63】



権利処理用のSAM105a

【図68】

Multi-SAM ID	
記録用鍵K _{SR} (Multi-Key)	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジット・デビット)	
電子マネー	
第3信頼機関(EMV・デビット)の公開鍵	
ホトCAの公開鍵	
Multi-SAM公開鍵証明書(X.509)	
Multi-SAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分算のための関連Multi-ID	
Multi-ID	
・Multiの種別情報	
・ROM/RAM	
イー・アイ・エフ物理アドレス情報 (ゼロ空間)	検証値
検証値(MAC)	
コピリライト-#10KF/KF1	
コピリライト-#20KF/KF1	
コピリライト-#30KF/KF1	
コピリライト-#40KF/KF1	
コピリライト-#50KF/KF1	
コピリライト-#60KF/KF1	
コピリライト-#70KF/KF1	
コピリライト-#80KF/KF1	
コピリライト-#90KF/KF1	
コピリライト-#100KF/KF1	
検証値(MAC)	

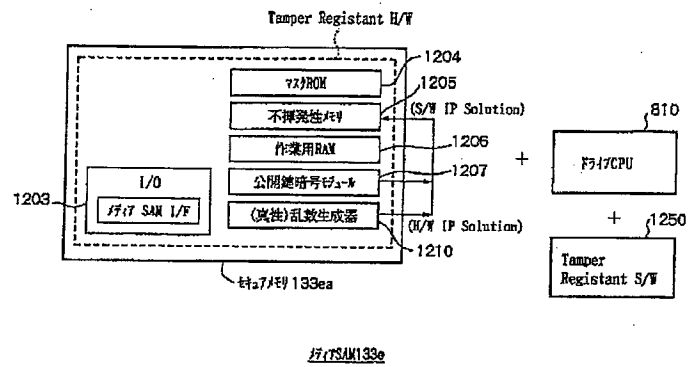
ROM記録媒体のMulti-SAM記憶データ(登録及び購入処理後)

【図70】

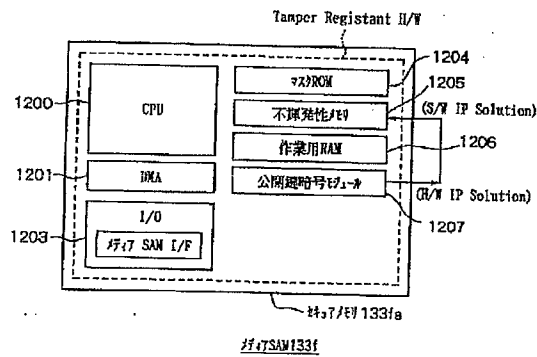
Multi-SAM ID	
記録用鍵K _{SR} (Multi-Key)	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジット・デビット)	
電子マネー	
第3信頼機関(EMV・デビット)の公開鍵	
ホトCAの公開鍵	
Multi-SAM公開鍵証明書(X.509)	
Multi-SAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分算のための関連Multi-ID	
Multi-ID	
・Multiの種別情報	
・ROM/RAM	
イー・アイ・エフ物理アドレス情報 (ゼロ空間)	検証値
検証値(MAC)	
コピリライト-#10KF/KF1	
コピリライト-#20KF/KF1	
コピリライト-#30KF/KF1	
コピリライト-#40KF/KF1	
コピリライト-#50KF/KF1	
コピリライト-#60KF/KF1	
コピリライト-#70KF/KF1	
コピリライト-#80KF/KF1	
コピリライト-#90KF/KF1	
コピリライト-#100KF/KF1	
検証値(MAC)	

RAM記録媒体のMulti-SAM記憶データ(登録及び購入処理後)

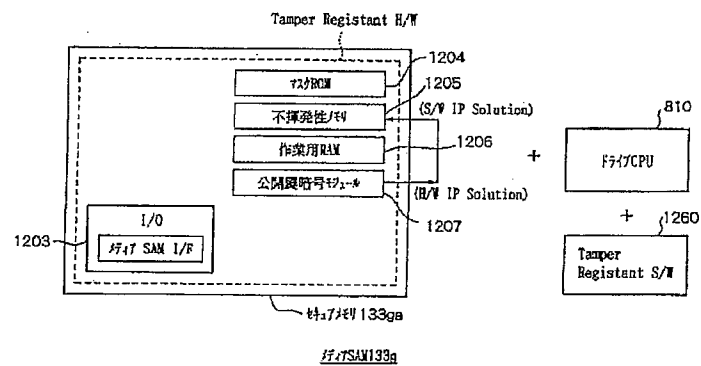
【図 7 4】



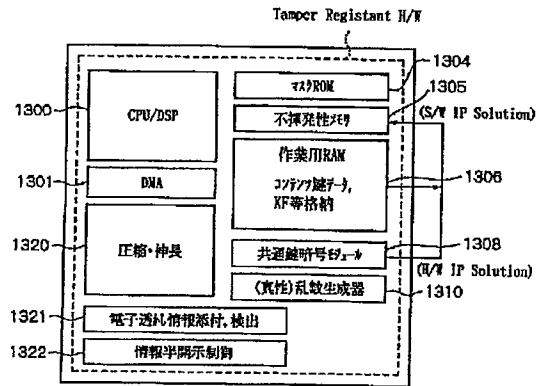
【図 7 5】



【図 7 6】

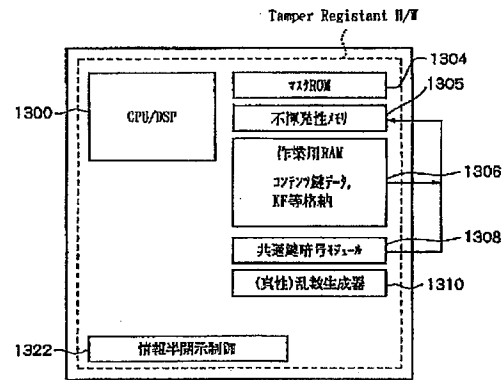


【図77】



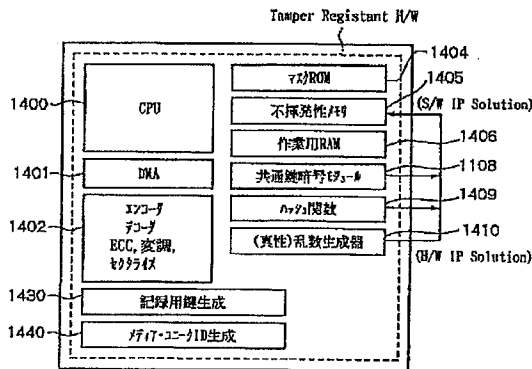
AVICチップ用SAM163

【図78】



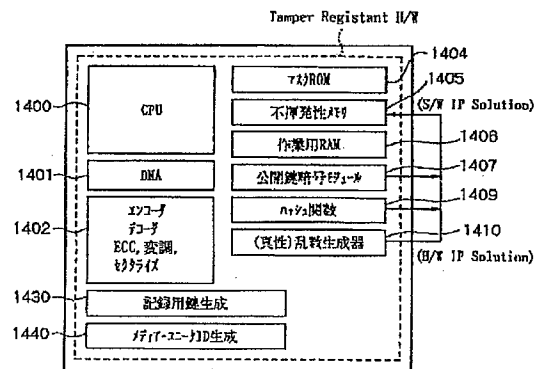
AVICチップ用SAM163

【図79】



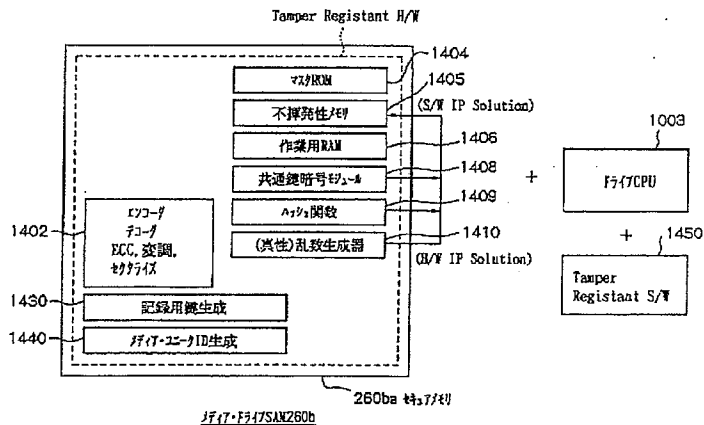
F347T・F347T SAM260a

【図80】



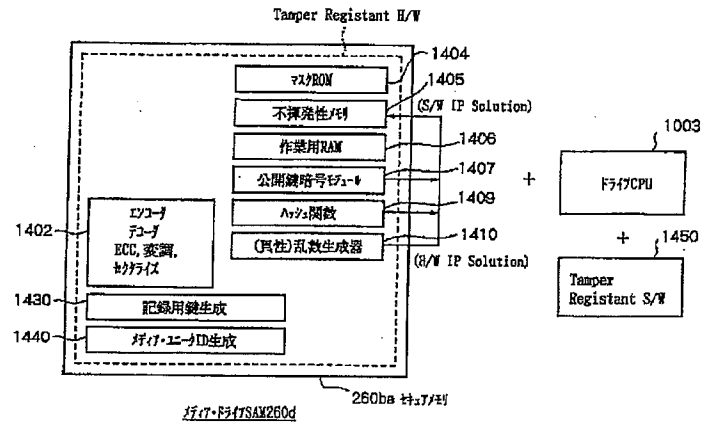
F347T・F347T SAM260c

【図81】

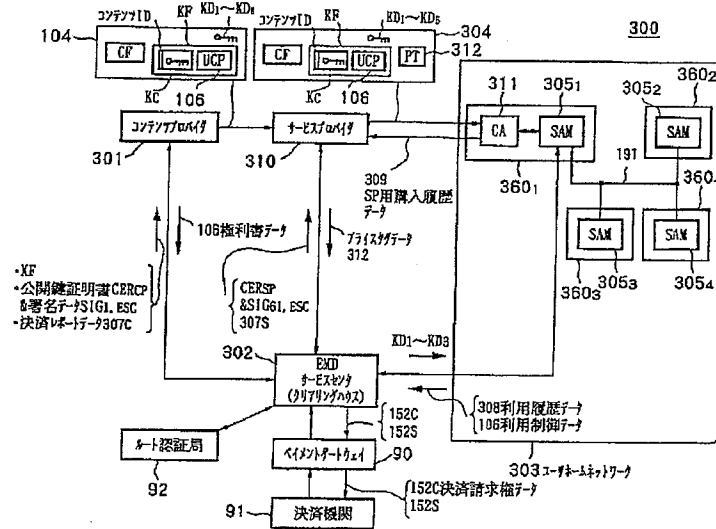


F347T・F347T SAM260b

【図82】



【図85】



【図83】

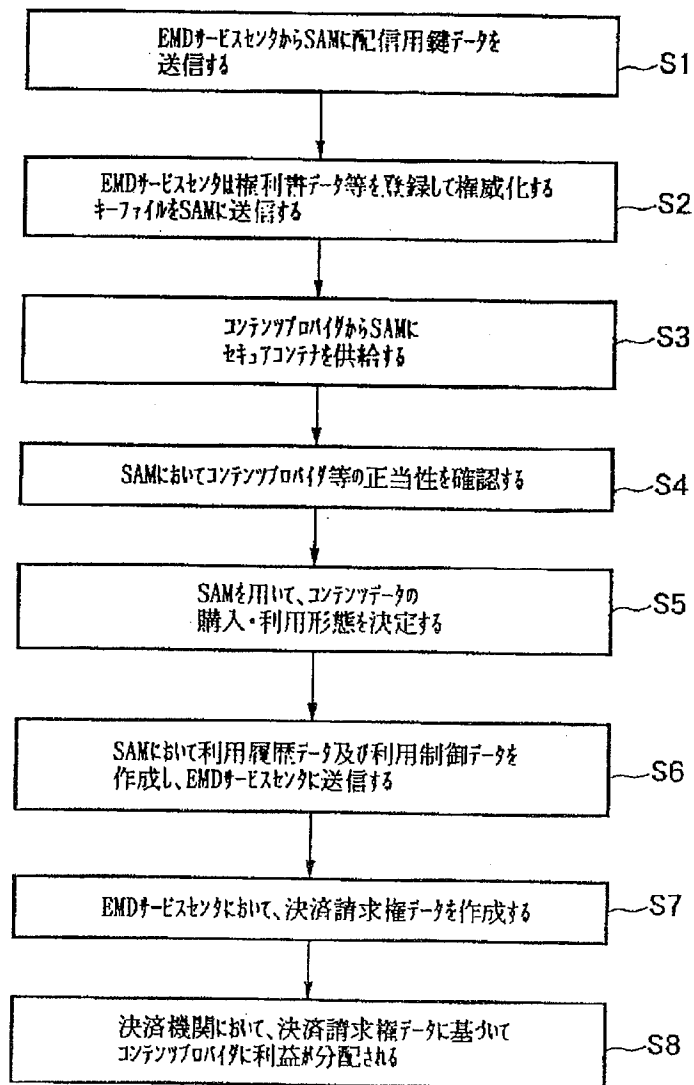


Figure 1 is a block diagram of a system architecture, labeled 100. The diagram illustrates the flow of data and control signals between various components.

Central Components:

- インターネット (Internet):** A central hub connecting different parts of the system.
- コンテンツサーバ 104 (Content Server 104):** A server that provides content to the system.
- インターネットロイヤリティ (Internet Royalty):** A block that manages royalty payments for content usage.

System Sections:

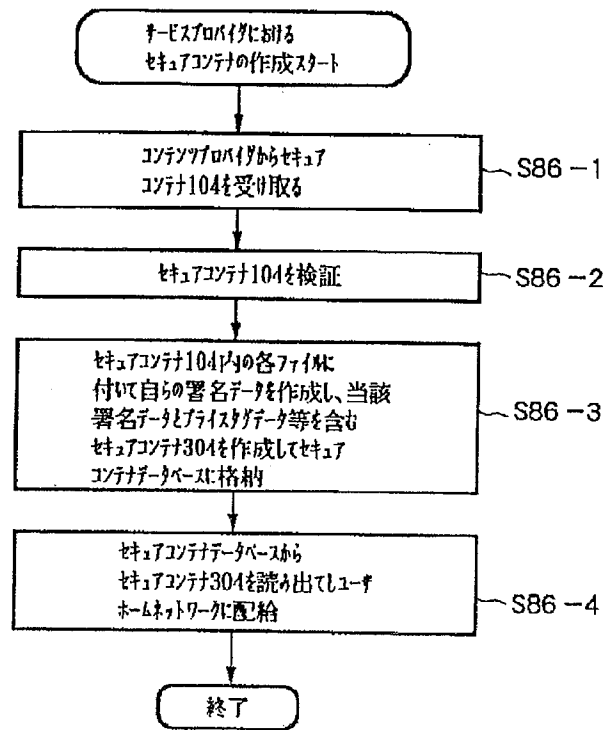
- インターネットロイヤリティ (101):** This section includes a **コンテンツサーバ 104** and a **インターネット** block. It is connected to the central Internet block.
- インターネットロイヤリティ (102):** This section includes a **コンテンツサーバ 104** and a **インターネット** block. It is connected to the central Internet block.
- インターネットロイヤリティ (103):** This section includes a **コンテンツサーバ 104** and a **インターネット** block. It is connected to the central Internet block.

External Connections and Processes:

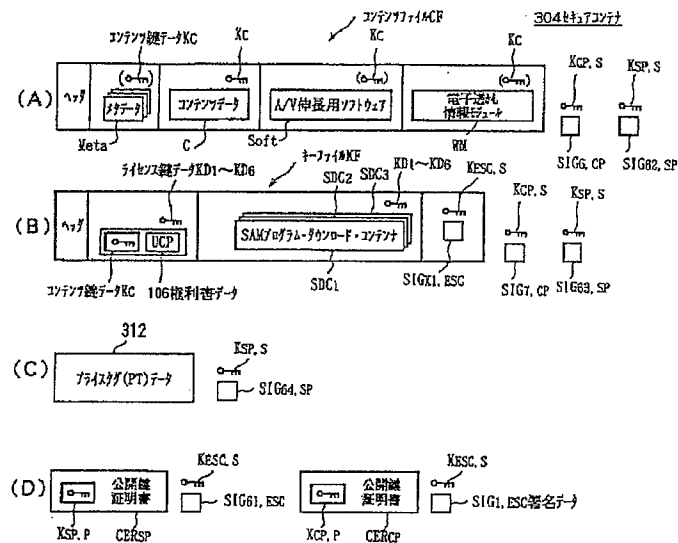
- コンテンツの権利登録 (Content Rights Registration):** A process that registers content rights with the system.
- コンテンツの権利利用 (Content Rights Usage):** A process that utilizes content rights within the system.
- インターネットロイヤリティ (101) to (103):** These blocks are connected to the central Internet block and manage royalty payments for content usage.
- インターネットロイヤリティ (101) to (103):** These blocks are connected to the central Internet block and manage royalty payments for content usage.

The diagram shows a complex network of connections between these components, indicating a highly integrated system for content distribution and royalty management.

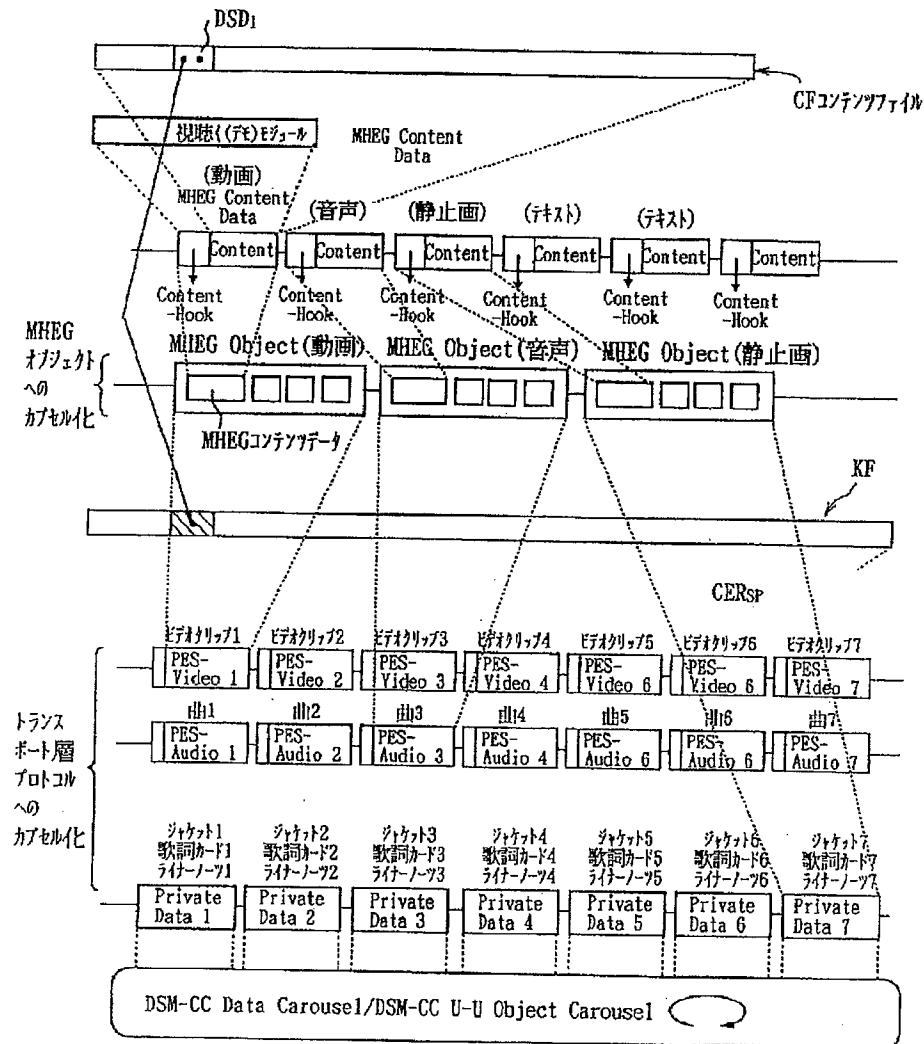
【図86】



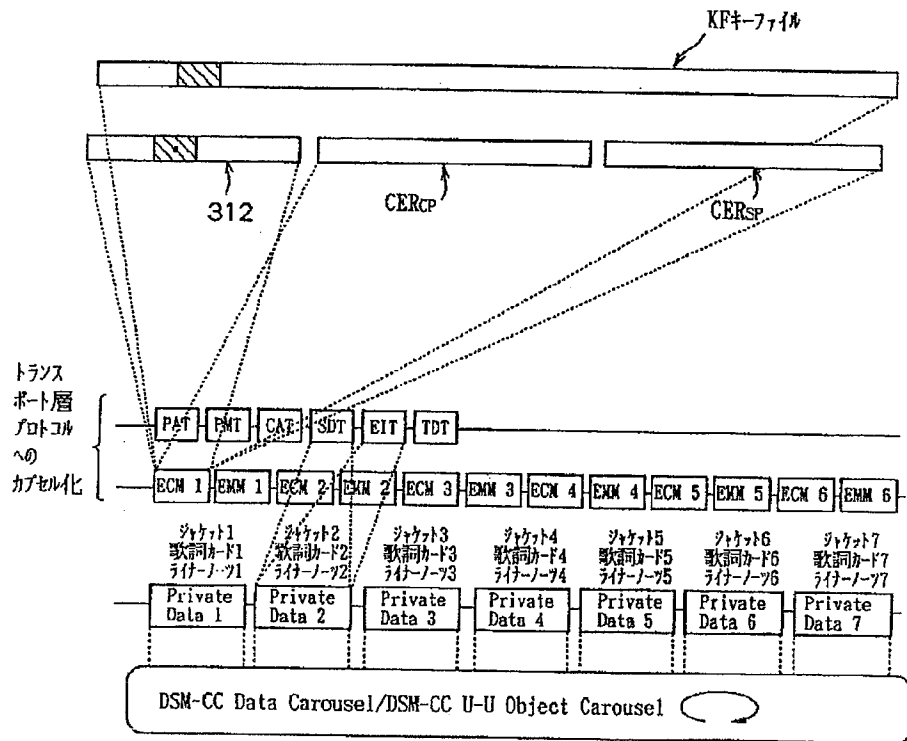
【図87】



【図88】



【図89】



【図90】

EMDサーステン302の主な機能

ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データDERCP, CERSP, CERSAM1〜CERSAM4の発行

キーファイルKFの生成

利用履歴データに基づく決済処理
(CPとSPとの間の利益分配処理)

3601



Figure 1 is a block diagram of a mobile station device 300. The device includes a communication unit 162, a baseband unit 308, a control unit 304, a mutual authentication unit 908, a memory unit 907, a signal processing unit 909, a signal processing unit 910, a signal processing unit 911, and an IC card 912. The device is connected to a base station 166 via a radio link 165. The device also includes a SIM 305 and a signal processing unit 304. The device is connected to a network 304 via a signal processing unit 304. The device is connected to a network 304 via a signal processing unit 304.

[illegible]

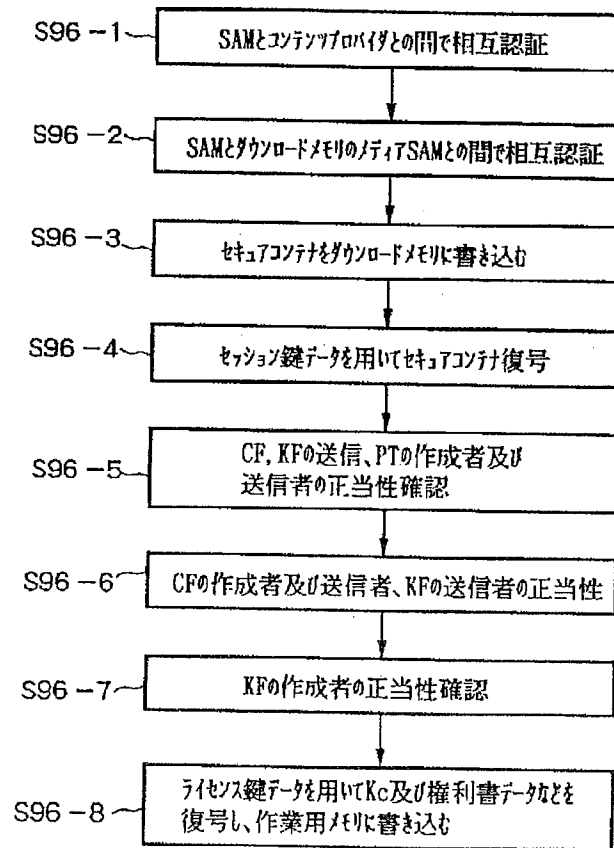
[illegible]

Figure 1 is a block diagram of a recording system. The system is divided into two main sections: a host system (top) and a recording medium (bottom).

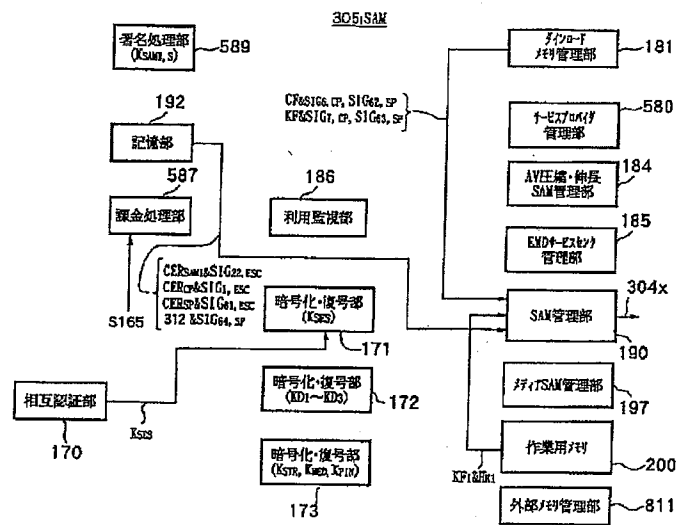
Host System (Top):

- 160:** Host system.
- 155:** CF utilization control unit.
- 304:** CF card.
- 305₁:** CF interface.
- 167:** CF controller.
- SAM:** SAM (Serial Access Memory) unit.
- CF:** CF (CompactFlash) interface.
- 161:** CF card.
- 162:** CF card.
- 163:** CF card.
- 164:** CF card.
- 165:** CF card.
- 166:** CF card.
- 167:** CF card.
- 168:** CF card.
- 169:** CF card.
- 170:** CF card.
- 171:** CF card.
- 172:** CF card.
- 173:** CF card.
- 174:** CF card.
- 175:** CF card.
- 176:** CF card.
- 177:** CF card.
- 178:** CF card.
- 179:** CF card.
- 180:** CF card.
- 181:** CF card.
- 182:** CF card.
- 183:** CF card.
- 184:** CF card.
- 185:** CF card.
- 186:** CF card.
- 187:** CF card.
- 188:** CF card.
- 189:** CF card.
- 190:** CF card.
- 191:** CF card.
- 192:** CF card.
- 193:** CF card.
- 194:** CF card.
- 195:** CF card.
- 196:** CF card.
- 197:** CF card.
- 198:** CF card.
- 199:** CF card.
- 200:** CF card.
- 201:** CF card.
- 202:** CF card.
- 203:** CF card.
- 204:** CF card.
- 205:** CF card.
- 206:** CF card.
- 207:** CF card.
- 208:** CF card.
- 209:** CF card.
- 210:** CF card.
- 211:** CF card.
- 212:** CF card.
- 213:** CF card.
- 214:** CF card.
- 215:** CF card.
- 216:** CF card.
- 217:** CF card.
- 218:** CF card.
- 219:** CF card.
- 220:** CF card.
- 221:** CF card.
- 222:** CF card.
- 223:** CF card.
- 224:** CF card.
- 225:** CF card.
- 226:** CF card.
- 227:** CF card.
- 228:** CF card.
- 229:** CF card.
- 230:** CF card.
- 231:** CF card.
- 232:** CF card.
- 233:** CF card.
- 234:** CF card.
- 235:** CF card.
- 236:** CF card.
- 237:** CF card.
- 238:** CF card.
- 239:** CF card.
- 240:** CF card.
- 241:** CF card.
- 242:** CF card.
- 243:** CF card.
- 244:** CF card.
- 245:** CF card.
- 246:** CF card.
- 247:** CF card.
- 248:** CF card.
- 249:** CF card.
- 250:** CF card.
- 251:** CF card.
- 252:** CF card.
- 253:** CF card.
- 254:** CF card.
- 255:** CF card.
- 256:** CF card.
- 257:** CF card.
- 258:** CF card.
- 259:** CF card.
- 260:** CF card.
- 261:** CF card.
- 262:** CF card.
- 263:** CF card.
- 264:** CF card.
- 265:** CF card.
- 266:** CF card.
- 267:** CF card.
- 268:** CF card.
- 269:** CF card.
- 270:** CF card.
- 271:** CF card.
- 272:** CF card.
- 273:** CF card.
- 274:** CF card.
- 275:** CF card.
- 276:** CF card.
- 277:** CF card.
- 278:** CF card.
- 279:** CF card.
- 280:** CF card.
- 281:** CF card.
- 282:** CF card.
- 283:** CF card.
- 284:** CF card.
- 285:** CF card.
- 286:** CF card.
- 287:** CF card.
- 288:** CF card.
- 289:** CF card.
- 290:** CF card.
- 291:** CF card.
- 292:** CF card.
- 293:** CF card.
- 294:** CF card.
- 295:** CF card.
- 296:** CF card.
- 297:** CF card.
- 298:** CF card.
- 299:** CF card.
- 300:** CF card.
- 301:** CF card.
- 302:** CF card.
- 303:** CF card.
- 304:** CF card.
- 305:** CF card.
- 306:** CF card.
- 307:** CF card.
- 308:** CF card.
- 309:** CF card.
- 310:** CF card.
- 311:** CF card.
- 312:** CF card.
- 313:** CF card.
- 314:** CF card.
- 315:** CF card.
- 316:** CF card.
- 317:** CF card.
- 318:** CF card.
- 319:** CF card.
- 320:** CF card.
- 321:** CF card.
- 322:** CF card.
- 323:** CF card.
- 324:** CF card.
- 325:** CF card.
- 326:** CF card.
- 327:** CF card.
- 328:** CF card.
- 329:** CF card.
- 330:** CF card.
- 331:** CF card.
- 332:** CF card.
- 333:** CF card.
- 334:** CF card.
- 335:** CF card.
- 336:** CF card.
- 337:** CF card.
- 338:** CF card.
- 339:** CF card.
- 340:** CF card.
- 341:** CF card.
- 342:** CF card.
- 343:** CF card.
- 344:** CF card.
- 345:** CF card.
- 346:** CF card.
- 347:** CF card.
- 348:** CF card.
- 349:** CF card.
- 350:** CF card.
- 351:** CF card.
- 352:** CF card.
- 353:** CF card.
- 354:** CF card.
- 355:** CF card.
- 356:** CF card.
- 357:** CF card.
- 358:** CF card.
- 359:** CF card.
- 360:** CF card.
- 361:** CF card.
- 362:** CF card.
- 363:** CF card.
- 364:** CF card.
- 365:** CF card.
- 366:** CF card.
- 367:** CF card.
- 368:** CF card.
- 369:** CF card.
- 370:** CF card.
- 371:** CF card.
- 372:** CF card.
- 373:** CF card.
- 374:** CF card.
- 375:** CF card.
- 376:** CF card.
- 377:** CF card.
- 378:** CF card.
- 379:** CF card.
- 380:** CF card.
- 381:** CF card.
- 382:** CF card.
- 383:** CF card.
- 384:** CF card.
- 385:** CF card.
- 386:** CF card.
- 387:** CF card.
- 388:** CF card.
- 389:** CF card.
- 390:** CF card.
- 391:** CF card.
- 392:** CF card.
- 393:** CF card.
- 394:** CF card.
- 395:</**

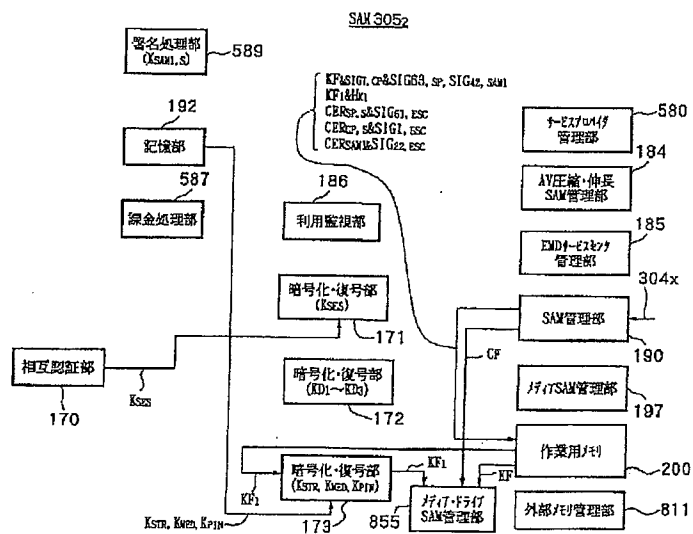
【図96】

セキュアコンテンツの入力処理(SAM)

【図98】

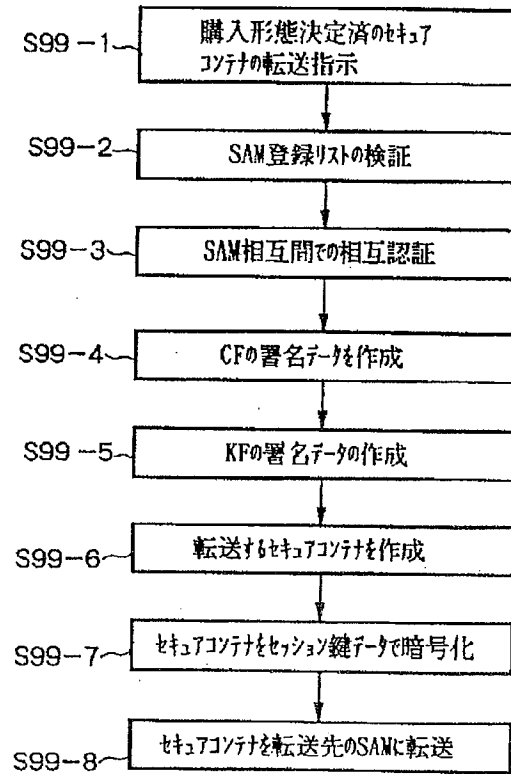


【図101】



【図99】

一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理



304xセキュリティ

(A) コンテンツ鍵データKC
Meta
ヘッダ
メタデータ
コンテンツデータ
KC
A/N伸長用ソフトウェア
Soft
電子透視情報システム
KC
KCP, S KSP, S KSAM1, S
SIG62, SP SIG41, SAM1

(B) ライセンス鍵データKD1~KD6
ヘッダ
LCP
106権利データ
KC
KC
KD1~KD6
SIG62, SP SIG41, SAM1
KCP, S KSP, S KSAM1, S

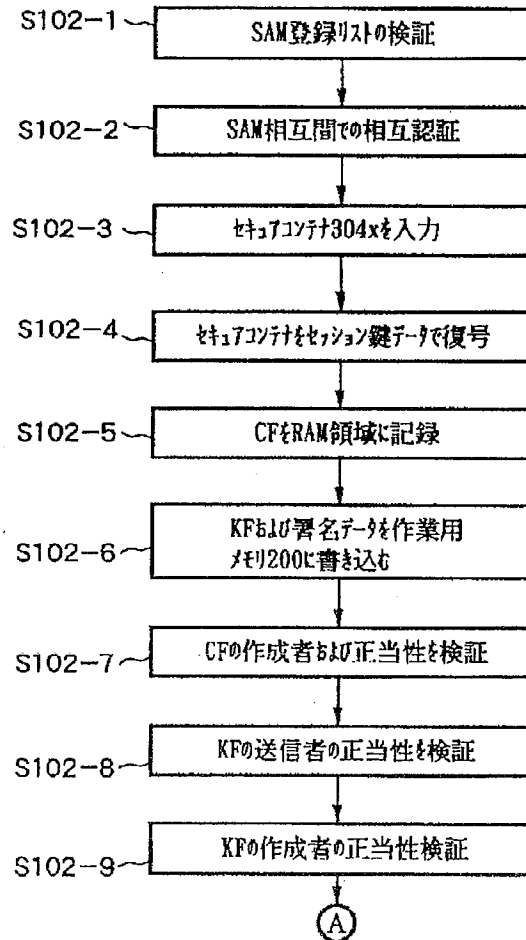
(C) コンテンツ鍵データKC
ヘッダ
UCP
166権利データ
KC
KD1~KD6
SIG62, SP SIG41, SAM1
KCP, S KSP, S KSAM1, S

(D) コンテンツ鍵データKC
ヘッダ
PTデータ
KC
KD1~KD6
SIG62, SP SIG41, SAM1
KCP, S KSP, S KSAM1, S

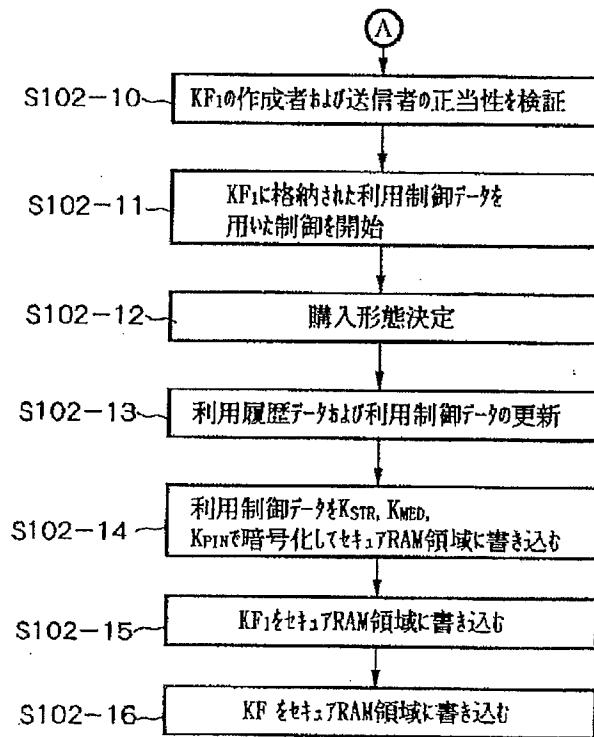
(E) 公開鍵証明書
ヘッダ
公開鍵証明書
KC
KD1~KD6
SIG62, SP SIG41, SAM1
KCP, S KSP, S KSAM1, S

【図102】

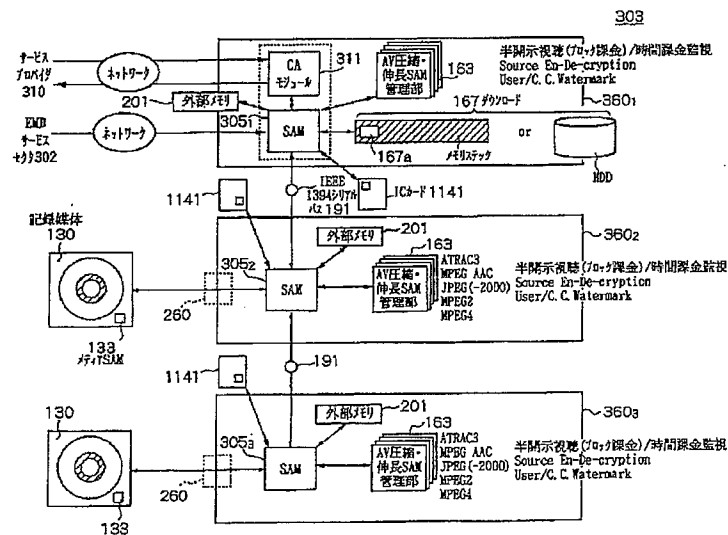
一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理



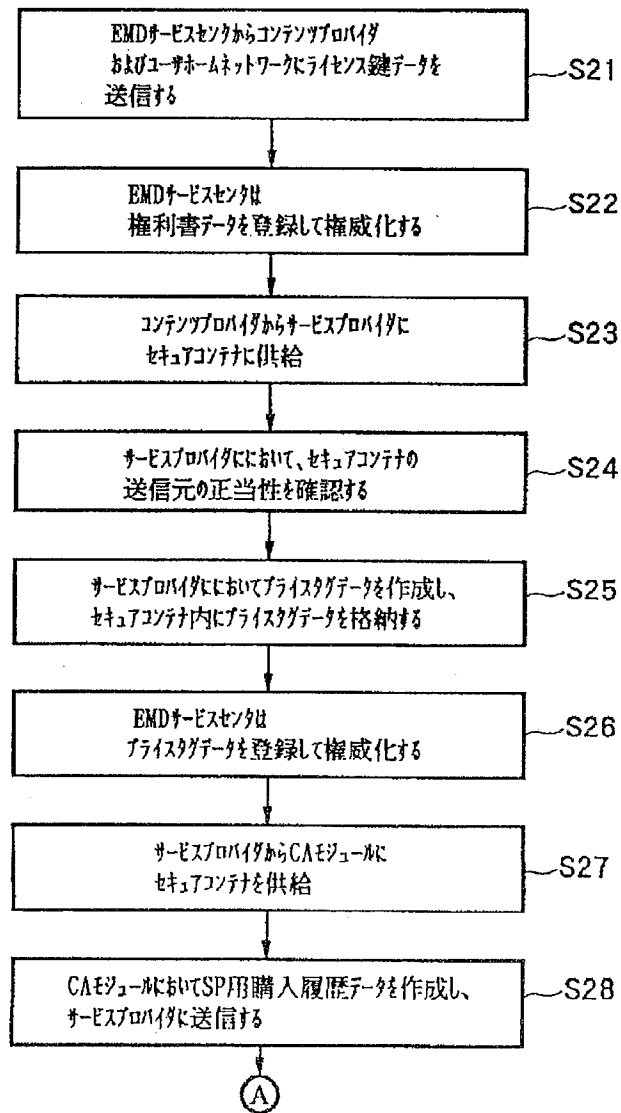
【図103】



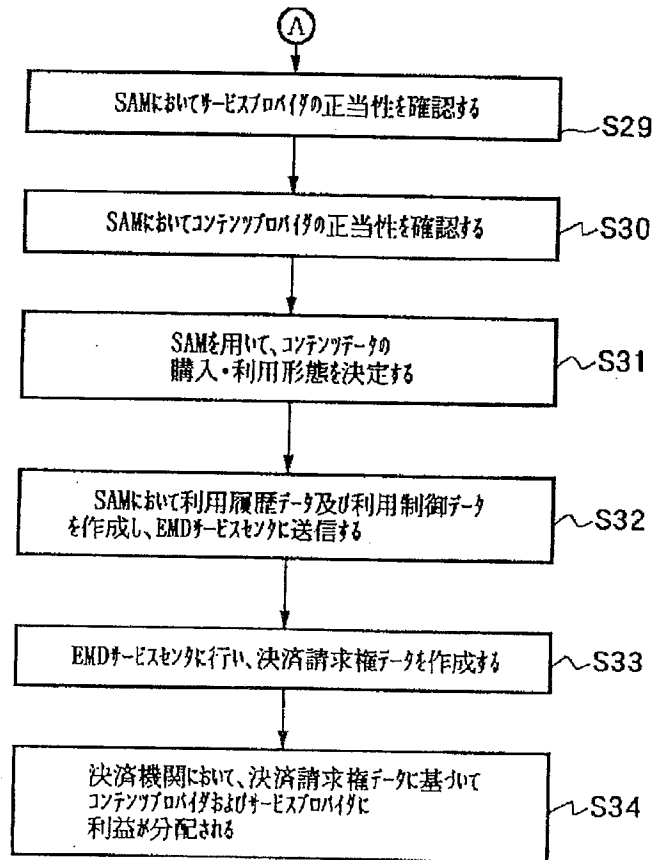
【図104】



【図105】

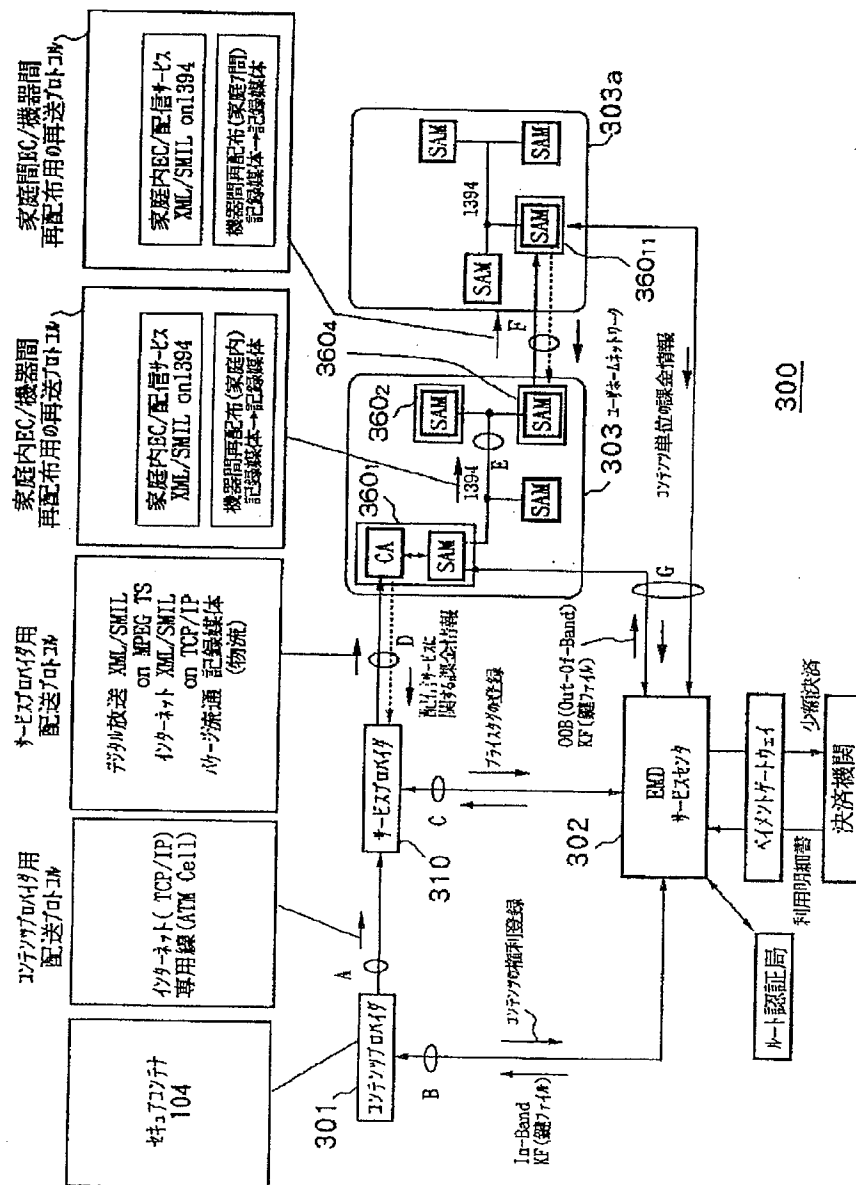


【図106】



[illegible]

300



Fターム(参考) 5B085 AG04 AE02 AE03 AE04 AE09
AE29
5G064 BA01 BB01 BB07 BC01 BC17
BC22 BD02 BD04 BD08
5J104 AA01 AA07 AA09 AA14 AA16
AA45 AA46 EA17 KA01 KA07
LA03 LA06 NA02 NA03 NA42
PA07 PA10 PA11
9A001 JJ19 JJ67 LL03

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第6部門第3区分
 【発行日】平成18年5月11日(2006.5.11)

【公開番号】特開2001-175605(P2001-175605A)
 【公開日】平成13年6月29日(2001.6.29)
 【出願番号】特願平11-359896
 【国際特許分類】

G 0 6 F 21/00 (2006.01)
 H 0 4 H 1/00 (2006.01)
 H 0 4 N 7/173 (2006.01)
 G 1 0 L 11/00 (2006.01)
 H 0 4 L 9/10 (2006.01)
 H 0 4 N 7/167 (2006.01)

【F 1】

G 0 6 F 15/00 3 3 0 Z
 H 0 4 H 1/00 F
 H 0 4 N 7/173 6 4 0 A
 G 1 0 L 9/00 E
 H 0 4 L 9/00 6 2 1 A
 H 0 4 N 7/167 Z

【手続補正書】
 【提出日】平成18年3月17日(2006.3.17)
 【手続補正1】
 【補正対象書類名】明細書
 【補正対象項目名】特許請求の範囲
 【補正方法】変更
 【補正の内容】
 【特許請求の範囲】

【請求項1】

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段と

を耐タンパ性の回路モジュール内に有する

データ処理装置。

【請求項2】

前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と

を前記耐タンパ性の回路モジュール内にさらに有する

請求項1に記載のデータ処理装置。

【請求項3】

前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらにを行い、

前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に
、前記決定を行う
請求項 1 に記載のデータ処理装置。

【請求項 4】

前記入力処理手段は、前記コンテンツデータの署名データを入力する処理をさらにに行い

前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に
、前記決定を行う
請求項 1 に記載のデータ処理装置。

【請求項 5】

前記入力処理手段は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利
書データのうち少なくとも一つのデータについて秘密鍵データを用いて作成された署名デ
ータと、前記秘密鍵データに対応する公開鍵データとを入力する処理をさらにに行い、

前記データ処理装置は、
前記公開鍵データを用いて、前記署名データの正当性を検証する署名処理手段を前記耐
タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に
、前記決定を行う
請求項 1 に記載のデータ処理装置。

【請求項 6】

前記コンテンツ鍵データは、ライセンス鍵データを用いて暗号化されており、
前記データ処理装置は、
前記ライセンス鍵データを記憶する記憶手段
をさらに有し、
前記復号手段は、前記記憶手段から読み出した前記ライセンス鍵データを用いて前記コ
ンテンツ鍵データを復号する
請求項 1 に記載のデータ処理装置。

【請求項 7】

前記データ処理装置は、他の装置との間で、前記コンテンツデータ、前記コンテンツ鍵
データおよび前記権利書データの少なくとも一のデータをオンラインで送受信する場合に
、前記他の装置との間で相互認証を行う相互認証手段と、
前記相互認証によって得られたセッション鍵データを用いて、前記送受信を行うデータ
の暗号化および復号を行う暗号化・復号手段と
を前記耐タンパ性の回路モジュール内にさらに有する
請求項 1 に記載のデータ処理装置。

【請求項 8】

コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データ
に基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、
当該データ処理装置の秘密鍵データを記憶する記憶回路と、
前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示
す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コン
テンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するた
めに、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性
を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項 9】

コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、

他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、

前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項 10】

ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】削除

【補正の内容】

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】削除

【補正の内容】

【手続補正 4】

【補正対象書類名】明細書
【補正対象項目名】0017
【補正方法】削除
【補正の内容】
【手続補正5】
【補正対象書類名】明細書
【補正対象項目名】0018
【補正方法】削除
【補正の内容】
【手続補正6】
【補正対象書類名】明細書
【補正対象項目名】0019
【補正方法】削除
【補正の内容】
【手続補正7】
【補正対象書類名】明細書
【補正対象項目名】0020
【補正方法】削除
【補正の内容】
【手続補正8】
【補正対象書類名】明細書
【補正対象項目名】0021
【補正方法】削除
【補正の内容】
【手続補正9】
【補正対象書類名】明細書
【補正対象項目名】0022
【補正方法】削除
【補正の内容】
【手続補正10】
【補正対象書類名】明細書
【補正対象項目名】0023
【補正方法】削除
【補正の内容】
【手続補正11】
【補正対象書類名】明細書
【補正対象項目名】0024
【補正方法】削除
【補正の内容】
【手続補正12】
【補正対象書類名】明細書
【補正対象項目名】0025
【補正方法】削除
【補正の内容】
【手続補正13】
【補正対象書類名】明細書
【補正対象項目名】0026
【補正方法】削除
【補正の内容】
【手続補正14】

【補正対象書類名】明細書
【補正対象項目名】0027
【補正方法】削除
【補正の内容】
【手続補正15】
【補正対象書類名】明細書
【補正対象項目名】0028
【補正方法】削除
【補正の内容】
【手続補正16】
【補正対象書類名】明細書
【補正対象項目名】0029
【補正方法】削除
【補正の内容】
【手続補正17】
【補正対象書類名】明細書
【補正対象項目名】0030
【補正方法】削除
【補正の内容】
【手続補正18】
【補正対象書類名】明細書
【補正対象項目名】0031
【補正方法】削除
【補正の内容】
【手続補正19】
【補正対象書類名】明細書
【補正対象項目名】0032
【補正方法】変更
【補正の内容】
【0032】

本発明のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有する。

【手続補正20】

【補正対象書類名】明細書
【補正対象項目名】0033
【補正方法】削除
【補正の内容】
【手続補正21】
【補正対象書類名】明細書
【補正対象項目名】0034
【補正方法】削除
【補正の内容】
【手続補正22】
【補正対象書類名】明細書
【補正対象項目名】0035
【補正方法】削除
【補正の内容】
【手続補正23】
【補正対象書類名】明細書
【補正対象項目名】0036
【補正方法】削除
【補正の内容】
【手続補正24】
【補正対象書類名】明細書
【補正対象項目名】0037
【補正方法】削除
【補正の内容】
【手続補正25】
【補正対象書類名】明細書
【補正対象項目名】0038
【補正方法】削除
【補正の内容】
【手続補正26】
【補正対象書類名】明細書
【補正対象項目名】0039
【補正方法】削除
【補正の内容】
【手続補正27】
【補正対象書類名】明細書
【補正対象項目名】0040
【補正方法】削除
【補正の内容】
【手続補正28】
【補正対象書類名】明細書
【補正対象項目名】0041
【補正方法】削除
【補正の内容】
【手続補正29】
【補正対象書類名】明細書
【補正対象項目名】0042
【補正方法】削除
【補正の内容】
【手続補正30】

【補正対象書類名】明細書
【補正対象項目名】0043
【補正方法】削除
【補正の内容】
【手続補正31】
【補正対象書類名】明細書
【補正対象項目名】0044
【補正方法】削除
【補正の内容】
【手続補正32】
【補正対象書類名】明細書
【補正対象項目名】0045
【補正方法】削除
【補正の内容】
【手続補正33】
【補正対象書類名】明細書
【補正対象項目名】0046
【補正方法】削除
【補正の内容】
【手続補正34】
【補正対象書類名】明細書
【補正対象項目名】0047
【補正方法】変更
【補正の内容】
【0047】

また、本発明のデータ処理装置は、コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有する。

【手続補正35】
【補正対象書類名】明細書
【補正対象項目名】0048
【補正方法】削除
【補正の内容】
【手続補正36】
【補正対象書類名】明細書
【補正対象項目名】0049
【補正方法】変更
【補正の内容】
【0049】

また、本発明のデータ処理装置は、ROM型またはRAM型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記

記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。

【手続補正 37】

【補正対象書類名】明細書

【補正対象項目名】0050

【補正方法】削除

【補正の内容】

【手続補正 38】

【補正対象書類名】明細書

【補正対象項目名】0051

【補正方法】削除

【補正の内容】

【手続補正 39】

【補正対象書類名】明細書

【補正対象項目名】0052

【補正方法】削除

【補正の内容】

【手続補正 40】

【補正対象書類名】明細書

【補正対象項目名】0053

【補正方法】削除

【補正の内容】